

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.
and
SAMSUNG ELECTRONICS AMERICA, INC.,
PETITIONER,

v.

SECURE WI-FI LLC,

PATENT OWNER.

U.S. PATENT NO. 9,961,552
ISSUED: MAY 01, 2018

ENTITLED: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

Inter Partes Review No.: IPR2024-01369

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

	Page
I. Mandatory Notices.....	1
A. Real Parties-In-Interest Pursuant to 37 C.F.R. § 42.8(b)(1).....	1
B. Related Matters Pursuant to 37 C.F.R. § 42.8(b)(2)	1
C. Lead and Back-Up Counsel Pursuant to 37 C.F.R. § 42.8(b)(3)	2
D. Service Information Pursuant to 37 C.F.R. § 42.8(b)(4).....	2
E. Payment of Fees under 37 C.F.R. §§ 42.15(a) and 42.103.....	3
II. Grounds for Standing.....	3
III. Preliminary Statement.....	3
IV. Identification Of Challenge	5
A. Prior Art.....	5
1. Vardi (EX1007, US8,126,476).....	5
2. IEEE802.11 (EX1009, IEEE Std 802.11TM-2012).....	6
3. Orava (EX1005, US2003/0177267)	8
4. Yun (EX1004, WO 2007/086705)	9
5. Kholaiif (EX1010, US2012/0257536).....	9
6. Motivation to Combine	10
B. Grounds for Challenge.....	20
V. The '552 Patent Overview	20
A. Applicants' Admitted Prior Art (AAPA).....	20
B. Alleged Invention of the '552 Patent in View of Prior Art	20
C. Prosecution History.....	23
D. Claim Construction	23
VI. Level of Ordinary Skill in the Art	23
VII. The Challenged Claims Are Unpatentable Over The Prior Art.....	24
A. Ground 1: Vardi in Combination with IEEE802.11, Orava, and Yun Render Obvious Claims 10-28	24
1. Independent Claim 10	24

2.	Claim 11: “The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.”	60
3.	Claim 12: “The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.”	61
4.	Claim 13: “The method of claim 10, further comprising: storing the authenticated access point list in a memory.”	61
5.	Claim 14	62
6.	Independent Claim 15	65
7.	Claim 16: “The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.”	70
8.	Claim 17: “The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.”	71
9.	Claim 18: “The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.”	72
10.	Claim 19: “The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.”	72
11.	Claim 20	73
12.	Independent Claim 21	74
13.	Claim 22: “The method of claim 21, wherein: the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and the fake device	

	identifier includes the fake media access control (MAC) address.”	75
14.	Claim 23: “The method of claim 21, further comprising: storing the fake device identifier in a memory.”	76
15.	Independent Claim 24	77
16.	Claim 25: “The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.”	83
17.	Claim 26: “The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.”	84
18.	Claim 27: “The system of claim 24, wherein the memory further stores the fake device identifier.”	85
19.	Claim 28: “The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.”	86
B.	Ground 2: 24-28 Are Obvious over Vardi in combination with IEEE802.11, Orava, and Kholaif.....	87
1.	Independent Claim 24	89
2.	Claim 25–Claim 27	92
3.	Claim 28	94
VIII.	Discretionary Denial Is Not Appropriate.....	95
A.	The Board Should Not Decline Institution Based on Fintiv.....	95
B.	The Board Should Not Decline Institution Based on General Plastic	98
C.	The Board Should Not Decline Institution Pursuant to §325(d)	99
IX.	Conclusion.....	99

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Comm’ns Techs., Inc. v. Samsung Elecs. Am., Inc.</i> , No. 2:21-cv-00444-JRG (E.D. Tex. Feb. 2, 2023).....	96
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	23, 24
<i>Sand Revolution II, LLC v. Continental Intermodal Group—Trucking LLC</i> , IPR2019-01393, Paper 24 (P.T.A.B. June 16, 2020)	97

Statutes

35 U.S.C.	
§ 102(a)	5
§ 102(b)	5, 9
§ 312(a)(3)	5

Other Authorities

37 C.F.R.	
§ 42.8(b)(1)	1
§ 42.8(b)(2)	1
§ 42.8(b)(3)	2
§ 42.8(b)(4)	2
§ 42.10(b)	2
§ 42.15(a)	3
§ 42.103	3
§ 42.104(a)	3

LISTING OF EXHIBITS

<u>Exhibit No.</u>	<u>Exhibit Title</u>
Exhibit 1001	U.S. Patent 9,961,552, filed May 01, 2018
Exhibit 1002	Declaration of Dr. Harry Bims
Exhibit 1003	Prosecution File History for U.S. Patent 9,961,552
Exhibit 1004	WO 2007/086705 (Yun), filed January 26, 2007
Exhibit 1005	US Patent Application Publication 2003/0177267 (Orava), filed December 5, 2002
Exhibit 1006	[RESERVED]
Exhibit 1007	U.S. Patent 8,126,476 (Vardi), filed July 25, 2008
Exhibit 1008	Microsoft Computer Dictionary 5 th Edition (Excerpts)
Exhibit 1009	IEEE Std 802.11TM-2012 (IEEE802.11), dated March 29, 2012
Exhibit 1010	US Application Publication 2012/0257536 (Kholaiif), filed April 8, 2011
Exhibit 1011	Infringement Contentions for U.S. Patent 9,961,552
Exhibit 1012	[RESERVED]
Exhibit 1013	[RESERVED]
Exhibit 1014	[RESERVED]
Exhibit 1015	[RESERVED]

CLAIM LISTING

Element Designation	Claim Language
Independent Claim 10	
10[pre]	10. A method performed by a device, the method comprising:
[10a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
[10b]	receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;
[10c]	transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;
[10d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
[10e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and
10[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 11	
[Claim 11]	The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.
Claim 12	
[Claim 12]	The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.
Claim 13	

[Claim 13]	The method of claim 10, further comprising: storing the authenticated access point list in a memory.
Claim 14	
14[pre]	14. The method of claim 10, further comprising:
14[a]	receiving, from the at least one access point, an approval of the connection request;
14[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
14[c]	receiving, from the at least one access point, an association response to the association request; and
14[d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 15	
15[pre]	15. A method performed by a device, the method comprising:
15[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
15[b]	generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
15[c]	transmitting, to at least one access point, a probe request frame that includes the fake device identifier;
15[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
15[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and

15[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 16	
[Claim 16]	The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.
Claim 17	
[Claim 17]	The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.
Claim 18	
[Claim 18]	The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.
Claim 19	
[Claim 19]	The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.
Claim 20	
20[pre]	The method of claim 15, further comprising:
[20a]	receiving, from the at least one access point, an approval of the connection request
[20b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
[20c]	receiving, from the at least one access point, an association response to the association request; and
[20d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 21	
21[pre]	A method performed by a device, the method comprising:
21[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

21[b]	generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;
21[c]	transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;
21[d]	receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
21[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and
21[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 22	
22[pre]	22. The method of claim 21, wherein:
22[a]	the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and
22[b]	the fake device identifier includes the fake media access control (MAC) address.
Claim 23	
[Claim 23]	The method of claim 21, further comprising: storing the fake device identifier in a memory.
Independent Claim 24	
24	A system, comprising:

24[a]	a processor;
24[b]	at least one communication interface;
24[c]	a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
24[d]	a receiver to:
24[d][i]	receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and
24[d][ii]	receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
24[e]	a memory to store the information regarding the at least one access point, and the authenticated access point list; and
24[f]	a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,
24[g]	wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and
24[h]	wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.
Claim 25	
[Claim 25]	The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.
Claim 26	
[Claim 26]	The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.
Claim 27	

[Claim 27]	The system of claim 24, wherein the memory further stores the fake device identifier.
Claim 28	
[Claim 28]	The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network

I. MANDATORY NOTICES

A. Real Parties-In-Interest Pursuant to 37 C.F.R. § 42.8(b)(1)

Petitioner Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively “Samsung”) are the real parties-in-interest.

B. Related Matters Pursuant to 37 C.F.R. § 42.8(b)(2)

Secure Wi-Fi (“SWF” or “PO”) filed a complaint alleging infringement of U.S. Patents 9,961,552 (the “’552 patent”), 9,971,005 (the “’005 patent”), and 10,694,384 (the “’384 patent”) (collectively, the “Asserted Patents”) against Samsung on January 25, 2024. That matter, *Secure Wi-Fi LLC v. Samsung Elecs. Co. Ltd. et al.*, No. 2:24-cv-00047-JRG in the Eastern District of Texas (the “Texas Action”), is currently pending. The Texas Action may affect, or be affected by, a decision in this proceeding.

The Asserted Patents are a family of patents sharing a specification. Petitioner is also petitioning for *inter partes* review against the ’005 (IPR2024-01366), ’384 (IPR2024-01367) patents and the remaining claims of the ’552 patent (IPR2024-01368). Petitioner will update its mandatory notices upon filing the challenges. Decisions in the ’005, ’384, and ’552 patents *inter partes* review proceedings may affect, or be affected by, a decision in this proceeding.

Currently, there are no other judicial or administrative matters that would affect, or be affected by, a decision in this proceeding.

C. Lead and Back-Up Counsel Pursuant to 37 C.F.R. § 42.8(b)(3)

Samsung identifies Walter D. Davis, Jr. (Reg. No. 45,137) as Lead Counsel and Dipu A. Doshi (Reg. No. 60,073), Jonathan W.S. England (Reg. No. 71,223), Sean Damon (*pro hac* forthcoming), and Arun Paradkar (Reg. No. 72,236) as Backup Counsel. Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition.

D. Service Information Pursuant to 37 C.F.R. § 42.8(b)(4)

Samsung identifies the following contact information of counsel in this proceeding.

Lead Counsel	
Walter D. Davis, Jr., (Reg. No. 45,137) BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006 Telephone: (202) 420-4847 Facsimile: (202) 478-0914 Email: walter.davis@blankrome.com	
Backup Counsel	
Dipu A. Doshi, (Reg. No. 60,073) Tel (202) 420-2604 Fax (202) 420-2201 dipu.doshi@blankrome.com	Sean D. Damon (<i>pro hac</i> to be filed) Telephone: (202) 420-4879 Facsimile: (202) 379-9380 Email: sean.damon@blankrome.com
Jonathan W.S. England, (Reg. No. 71,223) Telephone: (202) 420-2747 Facsimile: (202) 420-2201 Email: jonathan.england@blankrome.com	Arun Paradkar (Reg. No. 72,236) Telephone: (202) 772-5849 Facsimile: (202) 572-8439 Email: arun.paradkar@blankrome.com
BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006	BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006

Petitioner agrees to electronic service at the following email address:

Email: samsung-swf-iprs@blankrome.com

E. Payment of Fees under 37 C.F.R. §§ 42.15(a) and 42.103

The required fees are submitted herewith. If additional fees are owed during this proceeding, the PTO is authorized to charge Deposit Account No. [23-2185].

II. GROUNDS FOR STANDING

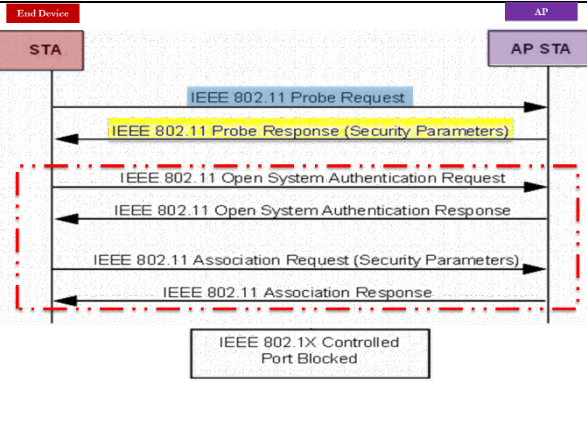
Pursuant to 37 C.F.R. § 42.104(a), Samsung certifies that the '552 Patent is available for *inter partes* review. Samsung is not barred or estopped from requesting *inter partes* review challenging the patent claim on the grounds set forth herein.

III. PRELIMINARY STATEMENT

Samsung petitions for *inter partes* review of claims 10-28 of the '552 patent.

The challenged claims are directed to methods and devices for wireless communication and relate to a particular procedure for connecting end devices to a wireless network.

Specifically, the patent discloses:

Summary of Asserted Claims	IEEE802.11 Active Scan
1. A device transmits a probe request with a Fake ID to an access point (“AP”) (defined by IEEE802). 2. Receiving a probe response from the AP, including information about the AP (“API”) (defined by IEEE802). 3. Determining whether the AP was previously connected to the device (defined by IEEE802). 4. Transmitting a connection request from the device to the AP (defined by IEEE802).	 The diagram illustrates the IEEE 802.11 Active Scan process between a Station (STA) and an Access Point Station (AP STA). The process is as follows: - The STA transmits an IEEE 802.11 Probe Request to the AP STA. - The AP STA responds with an IEEE 802.11 Probe Response (Security Parameters). - The STA then transmits an IEEE 802.11 Open System Authentication Request. - The AP STA responds with an IEEE 802.11 Open System Authentication Response. - The STA transmits an IEEE 802.11 Association Request (Security Parameters). - The AP STA responds with an IEEE 802.11 Association Response. - A box labeled IEEE 802.1X Controlled Port Blocked is shown below the association response, indicating a state where the port is blocked. Figure 4-17—Establishing the IEEE 802.11 association

The patented invention lacks the ingenuity and non-obviousness required for patent protection. The elements constituting this patent are simply a combination of well-known techniques and technologies readily apparent to a person of ordinary skilled in the art (POSITA). Indeed, the patent explains, “to connect to a wireless local area network (WLAN), an end device may search for at least one available access point around the end device. . . . When searching, the mobile device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device. . . . since the probe request frame that includes the device identifier is transmitted to access points around the end device, present location information of the end device may be exposed to some access points with which a user of the end device does not want to be connected....” EX1001, (3:4-16). The ’552 patent’s purported solution to the

“exposure”—a fake identifier. This exact procedure, however, was disclosed—by *Vardi*, *Orava*, and *Yun*—nearly a decade before.

As set forth below, claims 10-28 would have been obvious based on *Vardi* in view of *IEEE802.11*, *Orava*, and *Yun*.

IV. IDENTIFICATION OF CHALLENGE

A. Prior Art

All the prior art patents and printed publications discussed herein constitute prior art against the '552 patent under pre-AIA 35 U.S.C. §§ 102(a) or (b) and are submitted under 35 U.S.C. § 312(a)(3).

1. Vardi (EX1007, US8,126,476)

Vardi describes a system and method for connecting to access points by a user terminal or client in conjunction with a server stored database. EX1007, 3:4-6, 4:18-25, 4:43-57. *Vardi* discloses a database of access points that stores and collates information corresponding to the access points for its “clients” (*i.e.*, mobile devices) to utilize in real time. EX1007, 7:10-20, 7:33-36. The information stored and collected is based on prior connections between clients and access points and includes relevant information, including the MAC address and SSID of the previously-connected-to access points. EX1007, 3:21-30, 11:41-42. Clients continuously update the server based on their interaction and connection with the access points. EX1007, 3:4-6, 4:18-25 and 8:7-21. The server then updates its database and sends corresponding updates about relevant access points to its clients.

Id. Vardi explicitly discloses utilizing an IEEE 802.11 scan by its clients for active APs. EX1007, 10:34-36, 11:35-36, 13:4-7, 14:52-57. The client then compares the information received in the scan to the information it received from the database of preferred or favorite APs to determine which AP to connect to, including based upon previous connections and the AP information appearing in the database list. *Id.* Once the best access point is determined the mobile device can connect with the access point. *Id.*

2. IEEE802.11 (EX1009, IEEE Std 802.11TM-2012)

IEEE802.11 was published as a standard by the Institute of Electrical and Electronics Engineers (“IEEE”) in March 2012, and bears a 2012 Copyright date. The 2012 edition “gives users, in one document, the IEEE 802.11 standard for wireless local area networks (WLANS) with all the amendments that have been published to date.” By early 2012, IEEE802.11 was publicly available, well-known, and widely available to POSITAs. *See* [EX1002, Bims Expert Declaration (¶79) (“Bims”)] (explaining how “[a]t the time of its publication and afterwards, 802.11 was a well-known standard in the wireless industry specifying aspects of wireless local area networks (‘LANs’)”); EX1009, 1782 n.51 (“IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://www.standards.ieee.org/>).”). Thus, IEEE802.11 is prior art under at least §§102(a-b).

IEEE802.11 specifies “[t]he medium access control (MAC) and physical characteristics for wireless local area networks (LANs).” EX1009, iii. It describes the process by which mobile devices join and communicate with other stations. EX1009, 978. Specifically, the mobile device can use “Active scanning[, which] involves *the generation of Probe frames and the subsequent processing of received Probe Response frames.*” Bims, ¶¶79-82, EX1009, 978.

A typical *broadcast probe request* message seeks a response from *any* basic service set (BSS) and does not include the address of a specific SSID. *Id.*, 126. This is shown, in part, in Figure 10-3, which shows the scanning station issuing a broadcast probe message, and responder stations 1 and 2 issuing probe response messages:

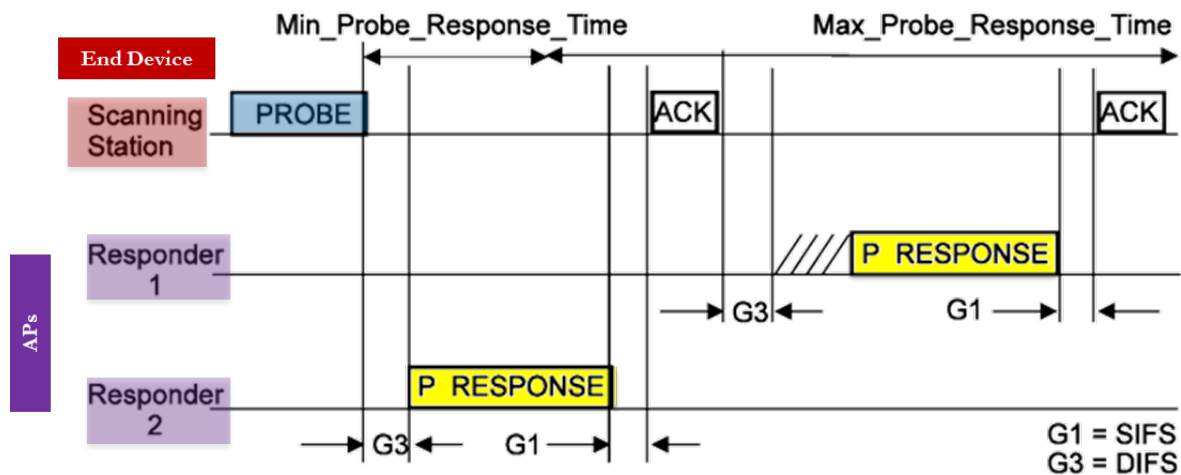


Figure 10-3—Probe response

If a device wishes to probe a specific BSS, for example a previously connected AP, then it *appends to the probe request message* the SSID of the specifically-

targeted BSS during the active scanning process. Bims, ¶83. Generally speaking, stations “receiving Probe Request frames shall respond with a probe response only if the SSID in the probe request is the broadcast SSID or matches the specific SSID of the STA.” EX1009, 979.

3. Orava (EX1005, US2003/0177267)

Orava discloses a system comprising “a terminal device MT and a WLAN network according to ***any version of the IEEE802.11 standard.***” *Id.*, ¶[19]. *Orava*, however, recognized that the use of fixed MAC addresses in IEEE 802.11 messages posed “a security risk: a MAC address can be picked up from every message transferred over the air interface... When the MAC address of the device is known, the movements of the device can be followed, and its traffic can be deliberately disturbed by causing collisions with packets by using a ‘stolen’ MAC address.” EX1005, ¶[03]. And *Orava*’s disclosures sought to put POSITAs on notice and teach them how to overcome this risk.

Thus, *Orava* provides procedures for generating and transmitting a random MAC address maintaining compliance with the 802.11 standard. EX1005, ¶[49]. It discloses the use of a random MAC address to facilitate a connection by a mobile terminal (“MT”) through an access point. EX1005, ¶[22]. But *Orava* also recognizes that it may only be advantageous to remain anonymous during the arrangement stage—during scanning—between the MT and AP. *Id.*, ¶[25]; Bims,

¶¶83-85. Not only does *Orava* provide a POSITA with numerous methods for generating an IEEE compliant random MAC address, *Id.*, ¶[30], *Orava* also, explains utilizing the random MAC address in the pertinent IEEE 802.11-based connection process, including scanning (active and passive), authentication, association, and subsequent connection to wireless devices. *Id.* at ¶¶[20], [29-31], and [49].

4. Yun (EX1004, WO 2007/086705)

Yun published on August 2, 2007, and is prior art under 35 U.S.C. § 102(b). EX1004, ¶[22]. *Yun* describes a wireless network system and communication methods for wireless networks. *Id.*, ¶[54].

Figures 4 and 5 illustrate the connection process for securely connecting the station to the WLAN, which corresponds to the connection process defined in *IEEE802.11*. *Id.*, Fig. 4, EX1009, 84 (Fig. 4-17).

To provide MAC address anonymity during probe requests transmissions, *Yun* describes using an arbitrary or random MAC address, identified as AMID, instead of the actual MAC address. *Id.*, ¶¶[144-145]. The station generates the AMID and then transmits a probe request including the AMID to the AP instead of the actual MAC address of the station. *Id.*, ¶[146], ¶¶[154-156].

5. Kholaiif (EX1010, US2012/0257536)

Kholaiif discloses configuring mobile stations for WLAN deployment. *Kholaiif* explains that the “various techniques disclosed in this document are... in the

context of IEEE 802.11-based wireless networking. This context is described in the IEEE 802.11 specifications for wireless local area network (WLAN) media access control (MAC) and Physical Layer (PHY).” EX1010, ¶[2]. And FIG. 27 provides “a functional block diagram illustration of an example mobile station.” EX1010, ¶[37].

6. Motivation to Combine

a. *Vardi, IEEE802.11, Orava, Yun*

Vardi teaches or at least suggests all the claimed 802.11 connection steps and components to perform those steps between a mobile device and access point (AP)—probing, authentication, and association. Although *Vardi* does not detail the underlying implementation of, for example, performing an “IEEE 802.11 scan,” “probing,” or “IEEE 802.11 association,” *Vardi* does explicitly disclose using IEEE802.11 to connect a mobile device and AP. Bims, ¶¶88-123. It therefore would have been obvious to a POSITA to look to *IEEE802.11* to provide the underlying details of *Vardi*’s “IEEE 802.11 scan,” “probing,” or “IEEE 802.11 association.” Bims, ¶¶88-123.

Indeed, each of *Vardi*, *Orava*, and *Yun* explicitly direct a POSITA to the standard to implement the disclosed systems and methods. EX1007, 7:36-43; EX1005, ¶[19]; EX1004, ¶[230]; Bims, ¶¶88-123.

Vardi alone discloses the well-known components required by claims 8-13. Specifically, *Vardi* discloses that a “*user terminal* can be a *device* that *executes a program... to find usable radio resources or wireless APs*,” “clients can continuously collect radio resource information about AP’s [sic] detected by the wireless terminal. These clients can be executed on laptops, handheld[] devices (PDA[s]), cellphones, or other devices that incorporate radio facility for wireless communication, such as WiFi,” a POSITA would understand this disclosure satisfies the claimed processor and communication interface including a transmitter and receiver. EX1007, 7:10-14, 9:54-59; Bims, ¶¶88-123.

Vardi discloses that “user’s clients can store... information in the memory of the wireless user terminal” and “can compare [received] scan result with its radio resource database to determine which APs are preferred for connection and roaming.” A POSITA would have readily understood these disclosures satisfying the claimed “memory” and “determination unit” components of the claims. EX1007, 7:31-32, 14:55-57; Bims, ¶¶88-123.

Vardi, however, does not disclose using a Fake ID. But what *Vardi* lacks—randomly generated Fake ID—*Orava* and *Yun* cover. Given the explicit teachings of *Orava* and *Yun* as IEEE802.11 compliant systems, it would have been obvious to a POSITA to apply *Orava*’s randomly generated Fake ID and *Yun*’s anonymous probe request transmission, while remaining IEEE802.11 compliant, to the *Vardi*

system. Bims, ¶¶88-123. Additionally, to the extent PO contends *Vardi* disclosures related to any of the hardware components are not explicit, *Orava* is explicit. It would have been obvious to a POSITA to implement *Vardi*'s system utilizing these well-known components of *Orava*.

First, *Vardi*, *Orava*, and *Yun* reference IEEE802.11 a **combined fifty-four times**. *Vardi*, *Orava*, and *Yun* provide a POSITA with a roadmap to implement their teachings as IEEE802.11 compliant and compatible systems. Bims, ¶¶88-123. To ensure proper formatting of the probe request/response messages that *Vardi*, *Orava*, and *Yun* disclose, a POSITA would have turned to the IEEE802.11 specification, which defines the probe request and probe response frame format.

Second, *Vardi*, *IEEE802.11 Orava*, *Yun*, and the '005 patent are all analogous art because they are directed to the same field of wireless communication using the IEEE 802.11 standard. See '552 patent, Abstract, 7:45-46; *Orava*, Abstract; EX1007, Abstract, 7:36-38; EX1004, ¶[230]; Bims, ¶¶88-123.

Third, *Orava* starts with *IEEE802.11*, identifies a problem, and seeks to solve the problem with a clear and explicit solution that remains IEEE802.11 compliant. EX1005, ¶¶[30], [49]. A POSITA would have been particularly motivated to look to *Orava*'s teachings to improve the *Vardi* communication system because *Orava*—a decade earlier than the '005 patent—described the problem with *Vardi* using manufacturer-assigned fixed MAC addresses. Specifically, *Orava* informed a

POSITA that “the fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message transferred over the air interface...” EX1005, ¶[3]. *Orava* also detailed the solution, “[i]n order to arrange anonymity, it has been suggested that *temporary random MAC addresses* be used for WLAN networks.” EX1005, ¶[4], ¶[29]

Although *Orava*’s solution provided numerous solutions for generating random fake identifiers, it did so using the *IEEE802.11* roadmap. EX1005, ¶[30] (“The IEEE 802 MAC address format allows locally administrable MAC address, in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.”); Bims, ¶¶88-123.

There were well-known benefits of using fake identifiers when establishing wireless communications. Bims, ¶¶88-123. Wireless communications (*e.g.*, Wi-Fi, 3G, 4G) that send messages over radio waves may be intercepted by unauthorized third parties. Encrypted communications ensure that only an authorized receiver can view the contents of the messages. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting their availability for a device to connect to their network.

As *Yun* teaches, enabling Wi-Fi connectivity to use a fake identifier before the connection phase with an access point before sharing the user’s private identifier would have prevented third-party attackers or unauthorized third parties from

compiling a list of SSIDs and private location information based on previously used hotspots. EX1004, ¶¶[154-156] (“*MAC address anonymity* makes an identity of the station not presumed through the MAC address... The transmitted packet on air uses an arbitrary MAC address(‘Dynamic MAC address’)... [the] invention relates to what protects the real MAC address of the station... the station *transmits* the ... *MAC address request such as the probe request*”); Bims, ¶¶88-123.

The IEEE 802.11 standard is the foundation of *Vardi’s*, *Orava’s*, and *Yun’s* teachings. For example, each utilize the IEEE 802.11 probe-request-response frame. Bims, ¶¶88-123; EX1007, 10:34-36 (“Basic *IEEE 802.11 association procedure*. . . using ... *probing* to get association information”), 7:36-40; EX1005, ¶[29] (“the terminal MT transmits a *Probe request*”), ¶[49] (“temporary MAC address can thus be used... in *all protocol messages*.”); EX1004, ¶[156] (“the station transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address Request’) to the access point. Because each system shares a foundational standard, it ensures interoperability between *Vardi*, *Orava*, and *Yun* for a POSITA with minimum effort and no undue experimentation. Bims, ¶¶88-123.

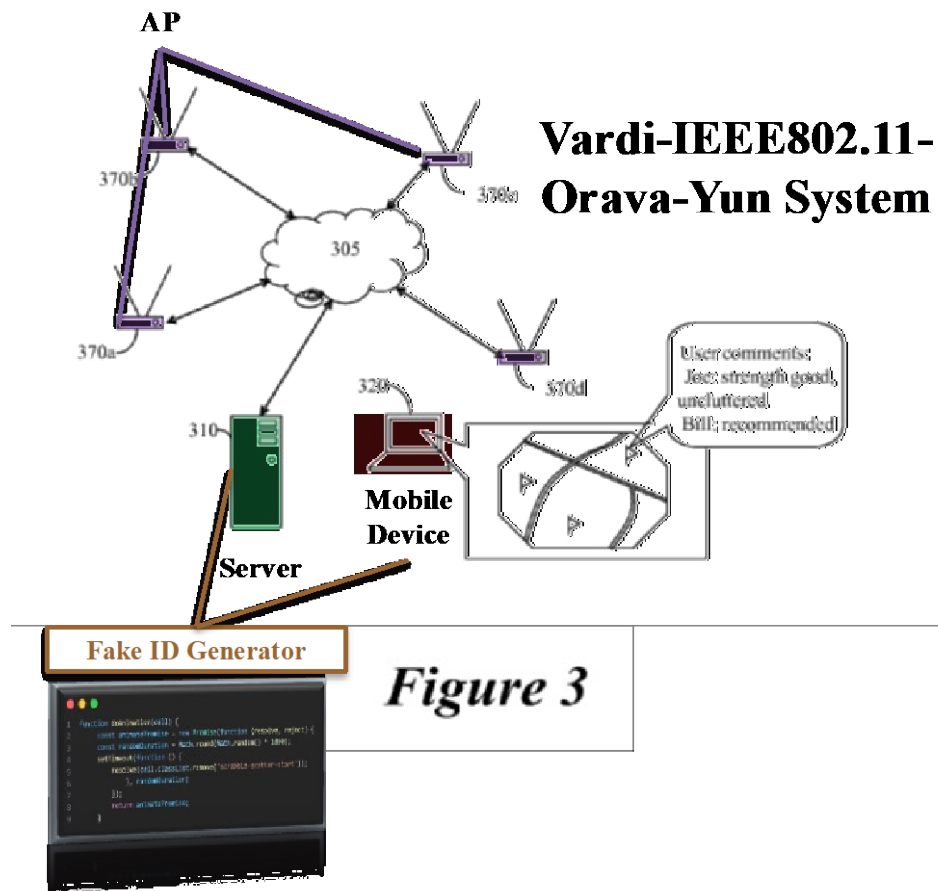
Lastly, a POSITA would have a reasonable expectation of success in applying *Orava’s* temporary MAC address teachings with transmitting in *Yun’s* probe request into *Vardi’s* wireless communication system because *Vardi’s* system already transmits probe messages including the MAC address as defined and taught by

IEEE802.11. A POSITA merely exchanges the probe request's real MAC address (also randomly generated by the manufacturer) for a temporarily generated random MAC address (Fake ID) to maintain interoperability. Bims, ¶¶88-123. Configuring *Vardi's* wireless system to substitute the "real" MAC address for *Orava's* temporary MAC address would have been a straightforward and routine application of well-known techniques in wireless communications. This straightforward and routine application is apparent because:

- (1) MAC addresses are themselves randomly generated per manufacturer, and thus randomly generating MAC addresses was well-known in the art;
- (2) *Vardi's* mobile device and server includes a processor and software to execute the random generation software;
- (3) it merely requires generating or receiving a random number or letter, plugging it into the standard IEEE 802.11 probe request frame without any modification to the standard or message format;
- (4) *Vardi's* server and mobile device are already configured to transmit data;
- (5) *Vardi* transmits probing messages to APs per IEEE802.11 standard; and
- (6) a POSITA would have been capable of implementing a temporary identifier within the existing system.

EX1007, 7:59-60; *EX1005*, ¶¶[3], [49]; *EX1004*, ¶¶[154-156]; Bims, ¶¶88-123.

In summary, *Vardi*, *Orava*, and *Yun* explicitly specify the use of *IEEE802.11*; thus, a POSITA would have naturally turned to the *IEEE802.11* standard for implementation details. At the same time, *Orava-Yun* provides the random MAC address generation functionality to minimize location tracking in the *Vardi* communication system and method (“*Vardi-IEEE802.11-Orava-Yun*”). Bims, ¶¶88-123.



b. *Vardi, IEEE802.11, Orava, Yun, and Kholaiif*

The *Vardi-IEEE802.11-Orava-Yun* system renders obvious claims 10-28. Despite the explicit disclosures above regarding well-known components of mobile devices at the time of the alleged invention, the PO may contend that the references do not disclose the connections between the components or within the mobile device. But *Kholaiif* does. EX1010, FIG. 27. A POSITA would have looked to and for components that support IEEE 802.11 standard communications when deploying mobile devices in an IEEE 802.11 WLAN. Bims, ¶¶124-130.

That is particularly true here, where *Kholaiif* also discloses selecting a target access point based on the results of a discovery scan, the type of network to which the access point provides access. EX1010, Abs., [52], [56], Fig. 2. The information used to select the desired access point includes the SSID. *Id.* at [90], [120]. *Kholaiif* further teaches an authentication process, including associating the mobile station with the target AP. *Id.* at Fig. 2, [49], [51], [59], [64-65], [69]. *Kholaiif* discloses the use of these techniques in the context of IEEE 802.11-based wireless networking. *Id.* at [2], [38]. *Kholaiif* also discloses a mobile station that can authenticate access points based on information about the access points, which includes a processor and a memory. *Id.* at [197], [242], [245].

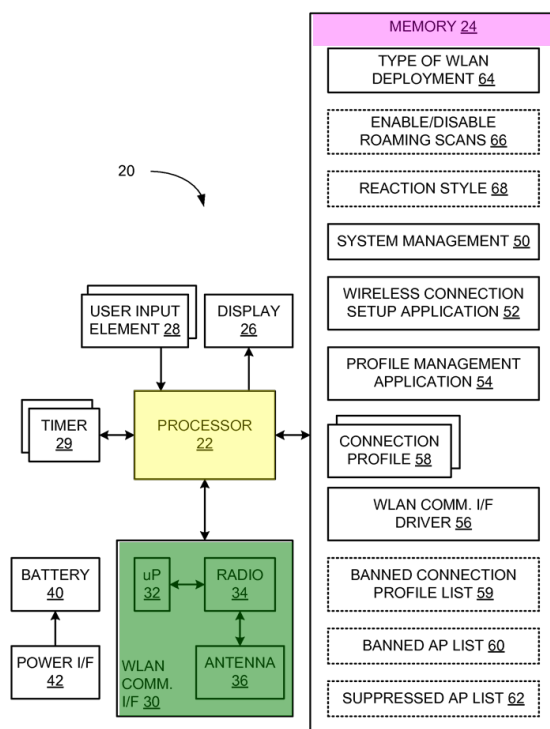


FIG. 27

Like *Vardi*, *IEEE802.11*, *Orava*, and *Yun*, *Kholaif* is also in the same field of endeavor as the '552 patent. The proposed combination would have been nothing more than (1) using known components, (2) inside known devices, (3) for their known purpose, (4) implementing a known standard for WLAN communication—the same IEEE802.11 standard.

A POSITA would have a reasonable expectation of success because using standardized supported components would have been common and expected. Bims, ¶¶124-130. Moreover, as explained above, *Vardi* and *Orava* disclose the same components and instructs a POSITA that the components need to be operable with IEEE802.11. Bims, ¶¶124-130.

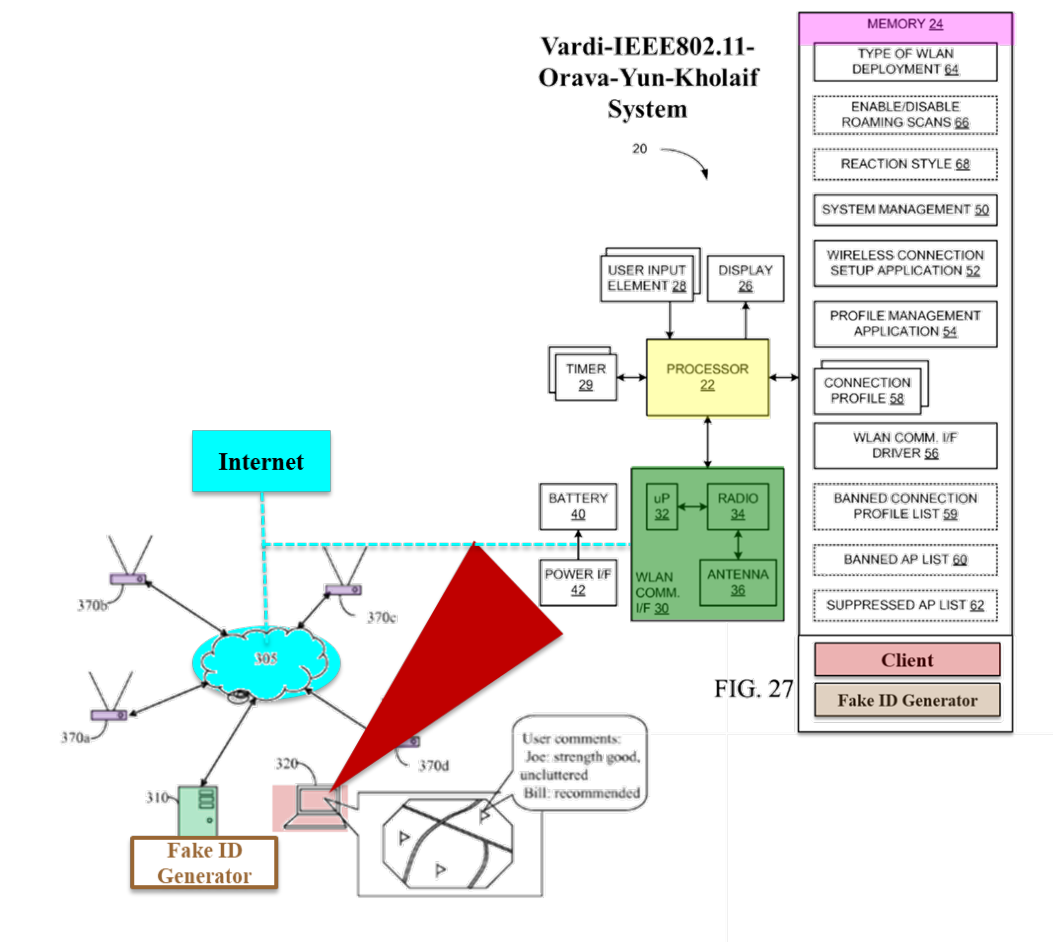


Figure 3

In summary, although a POSITA would have known that *Vardi*'s "clients [] execut[ing] on laptops, handheld devices, PDA's, cellphones, and other device[s] that incorporates a radio facility for wireless communication, such as Wifi," disclose the well-known components of claims 24-28; nonetheless, *Kholaif* discloses those components, and it would have been obvious to a POSITA to ensure these well-known components were implemented and would have done so successfully.

B. Grounds for Challenge

#	<u>Grounds</u>
1	Vardi, IEEE802.11, Orava and Yun renders obvious claims 10-28
2	Vardi, IEEE802.11, Orava, Yun, and Kholaf renders obvious claims 24-28

V. THE '552 PATENT OVERVIEW

A. Applicants' Admitted Prior Art (AAPA)

The '552 specification states, “to connect to a [] (WLAN), an end device may search for at least one available access point around the end device... the access point may be a Wi-Fi access point and the WLAN may be a Wi-Fi network. When searching, the end device may transmit a probe request frame that may include a device identifier, for the end device such as a [] (MAC) address of the end device... since the probe request frame that includes the device identifier is transmitted to access points around the end device, present location information of the end device may be exposed...” EX1001, 3:4-18.

B. Alleged Invention of the '552 Patent in View of Prior Art

The '552 patent is entitled SCHEMES FOR CONNECTING TO WIRELESS NETWORK and issued on May 1, 2018, claiming priority through intervening applications to International Application No. PCT/US2012/66306, filed on

November 21, 2012. EX1001 at (12), (45), (63). Therefore, for the purposes of this Petition, the earliest effective filing date of the '552 patent is November 21, 2012.

The '552 patent describes methods and devices configured to execute the described methods for secured wireless network communication scheme, generally between a mobile device, identified as an end device in the '552 patent, and a wireless network through a wireless access point. *See id.* at 3:1-4. Generally, the steps of the methods described in the '552 patent are shown in Fig. 4, reproduced below.

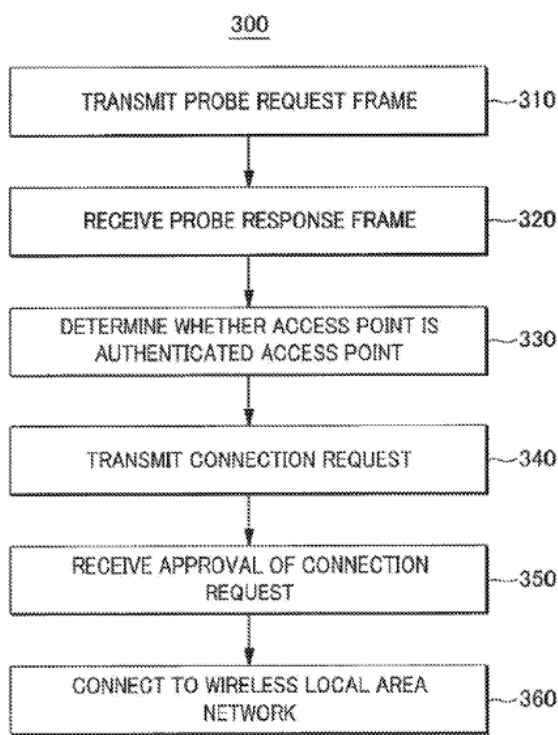


FIG. 3

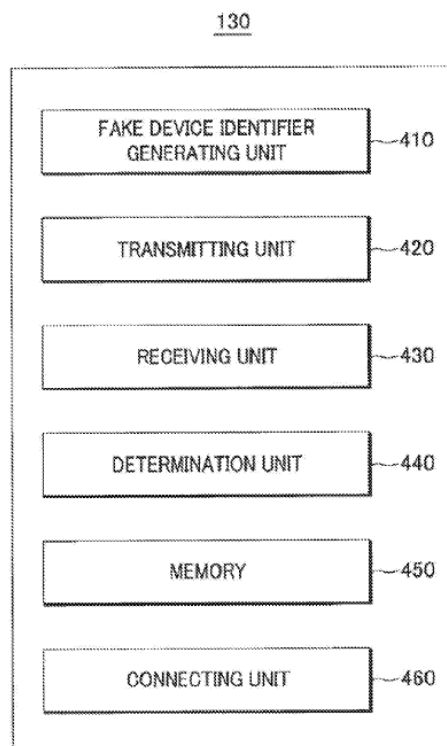


FIG. 4

Connecting to a wireless network, according to the '552 patent, can begin with the end device transmitting a probe request frame to all local access points. *Id.*, 3:8-

17. This step is in accordance with the IEEE Standard 2012. [EX1009, 82 (Fig. 4-17), §§4.3.8.2, 8.2.3, 8.3.3.9]. In the prior art, the probe request frame included an end device identifier, for example, an authentic MAC address for the end device. EX1001, 3:15-17. However, as identified by the '552 patent, by using the authentic MAC address of the end device in the public probe request frame transmission, present location information of the end device could be exposed to undesired access points where the user did not desire the authentic MAC address device identifier to be provided to. EX1001, 3:17-23.

To prevent such undesired disclosure of the authentic MAC address thereby disclosing present location information, the '552 patent teaches transmitting a fake device identifier instead of the authentic device identifier within the probe request frame. EX1001, 3:24-27, 4:4-16. The '552 patent teaches that the end device can generate or obtain the fake device identifier, which may include one random number or random character therein. EX1001, 4:4-16.

The remaining disclosures of the '552 patent track the IEEE Standard 2012, receiving from an access point, a probe response frame. EX1001, 3:27-29; IEEE802.11 [IEEE Standard 2012 at §§8.2.5.7, 8.3.3.10, Table 8-27), 82 (Fig. 4-17)]. Transmitting an authentication request after receiving a probe response is also in accordance with the IEEE Standard 2012. EX1009, §§4.10.3.1, 4.10.3.2, 84 (Fig. 4-17), 92, 98, 380, 818, 929.

C. Prosecution History

The application that issued as the '552 patent was filed on April 22, 2015, and is a continuation of application Ser. No. 13/885,754, filed May 16, 2013, now U.S. Pat. No. 9,717,005, which is a U.S. Natl. Stage filing of International Appl. No. PCT/US12/66306.

D. Claim Construction

Claims must be construed only to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Here, no terms need construction to resolve the controversy in this forum.¹

VI. LEVEL OF ORDINARY SKILL IN THE ART

Samsung submits that a POSITA for the '552 patent would have had a degree in computer engineering, computer science, or a similar discipline, along with 2 years of professional experience in the fields of networking and network-based systems or applications, or an equivalent level of skill, knowledge, and experience. And would be aware of and generally knowledgeable about how devices were provisioned onto wireless networks, along with standards applicable to well-known methods for communication such as Wi-Fi, Bluetooth, and 3G available at the time

¹ Petitioner reserves the right to argue in an appropriate forum that certain limitations in the challenged claims are indefinite.

the '552 Patent was filed. Bims, ¶¶36. Relevant graduate education could substitute for professional work experience. *Id.*

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE OVER THE PRIOR ART

A. Ground 1: *Vardi* in Combination with *IEEE802.11*, *Orava*, and *Yun* Render Obvious Claims 10-28

1. Independent Claim 10

- a. 10[pre]: “*A method performed by a device, the method comprising:*”

Vardi discloses a wireless communication system where the **user terminal** performs a method for connecting to the Internet via an **access point** using **access point information** (“API”) it received from the **server**. EX1007, 3:11-13, 6:49-54 (“the inventive method and system...”), 4:18-27, 4:42-48, FIGS. 1-3² Bims, ¶¶133-136, 37-57.

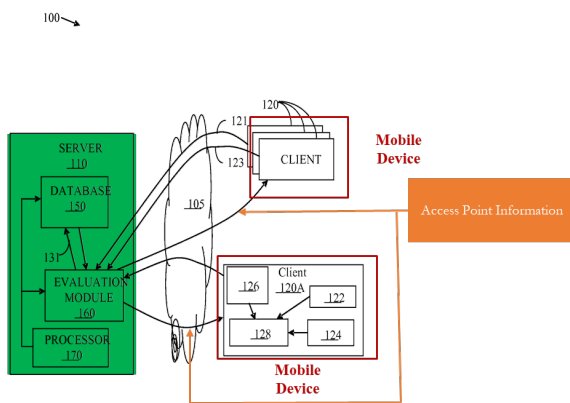


Figure 1

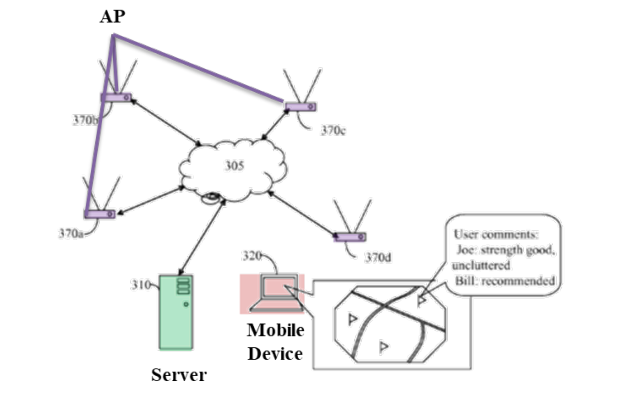


Figure 3

² All annotations added unless explicitly stated otherwise.

- b. 10[a]: “receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;”

Vardi-IEEE802.11-Orava-Yun render obvious this limitation. Bims, ¶¶330-375. FIG. 2 of the ’552 patent “shows an illustrative example of an authenticated access point list.”³ The corresponding specification indicates what the list may include—SSID or MAC address. EX1001, 4:37-45. PO’s infringement contentions add that it’s the SSID or MAC address of a **previously connected AP**. EX1011, 22. Regardless of whether the lists include SSIDs or MAC addresses of newly discovered or previously connected **APs**, *Vardi* teaches or suggests it.

As detailed below, *Vardi* discloses that **mobile devices** receive an authenticated access point list from a server. The list includes **information about the access point(s)** (“**API**”)—including the SSID and MAC address—of APs controlled by the server and the list is stored in memory. Bims, ¶¶330-375; EX1007, FIG. 1; 3:4-6, 25-54.

Receiving, from a server, an authenticated access point list that includes information regarding an access point. *Vardi* discloses **mobile devices** “executes

³ Petitioner reserves the right to argue in an appropriate forum that certain limitations in the challenged claims are indefinite.

a program (e.g., a **client**) that uses the combined data to find usable **radio resources** or **wireless APs** and establishes network connections through them, for example connections to the internet.” 7:10-14. *Vardi*’s mobile devices utilize the received **API** to compare with the stored **API** to select and connect to their preferred AP—authenticated access point. Specifically, *Vardi*’s “**clients** receive updates about **relevant access points** from the **server** and use **the information** to **select** and **connect** to the **preferred access point**.” 3:4-6. The **API** “can include **access point connectivity information** that can be used by the **wireless user terminal** to connect to the **access point**.” 3:25-59 (e.g., **API** illustrated below), 7:23-32 (access point **connection or connectivity data** stored in memory), 12:24-30 (cache information related to previously connected APs), 13:13-23 (compare received API with stored API to connect to “‘**favorite**’ AP.”); Bims, ¶¶330-375.

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

Vardi teaches the received list is an “authenticated access point list” under either interpretation—new or previously connected APs—because the mobile devices provide continuous updates to the server regarding APs in the vicinity, which the server “stor[es] the information about each access point in one or more databases,” evaluates the information, and “if the information is different or if additional information can be inferred” the information “can be sent to one or more user terminals and used by each user terminal to select a preferred radio resource for connection.” 3:11-26. *Vardi* discloses that the mobile device stores the received API in memory. EX1007, 7:23-32, 12:24-39, 13:13-23. Bims, ¶¶330-375.

Thus, the API includes the SSID and MAC address of newly discovered APs and the device’s previously connected APs. Bims, ¶¶330-375. Furthermore, *Vardi* details that “[i]f a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client)... is detected by the IEEE 802.11 scan... the client can select this AP for connection...” 13:13-17; Bims, ¶¶330-375.

Indeed, *Vardi* discloses that “it is well known in prior art computing systems to cache information related to an access point to which the mobile device has connected before. . . when the mobile device is activated at a later time in the same locale, the system uses the information in the cache to automatically reconnect to that AP. The cache normally includes the name and the MAC address of the AP.” EX1007, 12:24-30; Bims, ¶¶330-375.

The received API includes information on APs controlled by the server⁴.

The only reference to “controlled by the server” in the specification of the ’552 patent is to indicate that “the authenticated access point may include an access point controlled by mobile operating server.” EX1001, 4:33-35. Beyond this language, the specification does not detail what it means to be “controlled by the server.”

Looking at the claims, claim 24 recites “wherein to determine the... access point is... under control of the server, the determination unit determines whether the information regarding the... access point is *included in the authenticated access point list*.” Accordingly, claim 24 indicates that APs are under the server’s control if they are “included in the authenticated access point list.” EX1001, cl. 24.

Vardi discloses that the mobile device determines whether the AP is the preferred AP—an authenticated access point—by comparing the stored API with the API received from an IEEE802.11 scan. EX1007, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can *compare this scan result with its radio resource database* [the claimed “authenticated access point list” in

⁴ Petitioner reserves the right to argue in an appropriate forum that certain limitations in the challenged claims are indefinite.

memory] to determine which APs are preferred for connection...”); Bims, ¶¶330-375.

Separately, if PO contends that controlled by the server means that the server can send a request and receive a response from the AP, *Vardi* discloses this too. *Vardi* discloses, “**Server** can also include an evaluation module, which can *evaluate[] accessibility, bandwidth and other characteristics of various AP[s]*, and store the information as an update in database...,” EX1007, 7:53-58, subsequently the **server** transmits the **stored information** to the **device(s)**. Bims, ¶¶330-375. Additionally, *Vardi* teaches that the “**server** can include MappingType information that indicates the method by which the AP was mapped... where the **server** or the client *receives information about the location of an AP using two or more different methods of mapping*, location determination using one method can be selected to take precedence...” EX1007, 16:47-54.

To the extent the PO contends “controlled by the server” means something else, *Vardi* also discloses this feature when applying PO’s infringement contention theory. PO’s contentions allege:

The access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generating by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server.

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

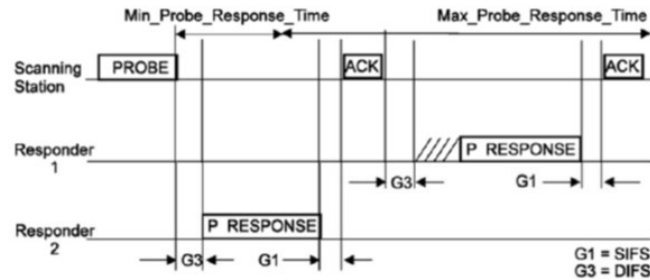


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

EX1011, 22.⁵

Vardi discloses the same probe request/response communication depicted in PO's infringement contentions, including the SSID and MAC address. *Vardi* explains the **mobile device** can perform a "Basis IEEE 802.11 association procedure... using... *probing* to *get association information*" and "*information acquired as part of the standard 802.11 scan, i.e., [Network or AP name (SSID—service set identifier); and, AP Radio Mac address]*" is included in the response from the **AP**. 10:25-36, 7:10-46, 9:54-64; Bims, ¶¶330-375.

⁵ PO's infringement contention contradicts PO's prosecution position.

Further, under PO's infringement theory, *Vardi* teaches or at least renders obvious that the APs are under control of the server because *Vardi*'s "clients receive updates about relevant access points from the server and use the information to select and connect to the preferred access point." EX1007, 3:4-6. That is, the "information" about the "relevant access points" is used by *Vardi*'s mobile device to perform a "Basic IEEE 802.11 association procedure... using probing to get association information" and "connect to the preferred access point." EX1007, 10:34-36; Bims, ¶¶330-375.

A POSITA would have readily understood at the time of the alleged invention that *Vardi*'s express recitation of "probing" and "standard 802.11 scan" is (1) the same probe request/response communication identified in PO's infringement contentions and (2) defined by IEEE802.11. Bims, ¶¶330-375. Additionally, PO's infringement theory relies upon the IEEE standard as evidence of infringement, EX1011, 22; however, the IEEE802.11 standard (EX1009) is prior art. Thus, if IEEE802.11's probe request/response infringes, it also invalidates the claim.

However, to the extent that the PO contends that *Vardi*'s disclosure of "probing" is not explicit, IEEE802.11 discloses (and defines) the "Active scan" procedure of *Vardi* as depicted below. During an active scan, the mobile device sends a probe request to various APs, and in response, the APs send a probe

response, including API, which includes both the SSID and MAC address of the AP.

Bims, ¶¶330-375, 37-57.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

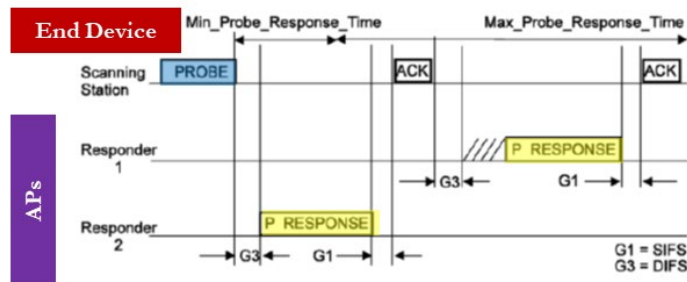


Figure 10-3—Probe response

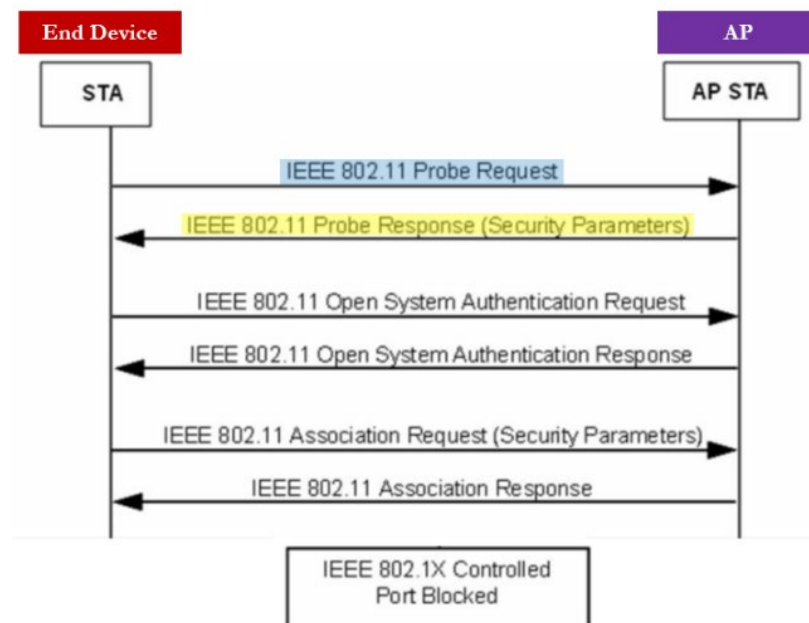


Figure 4-17—Establishing the IEEE 802.11 association

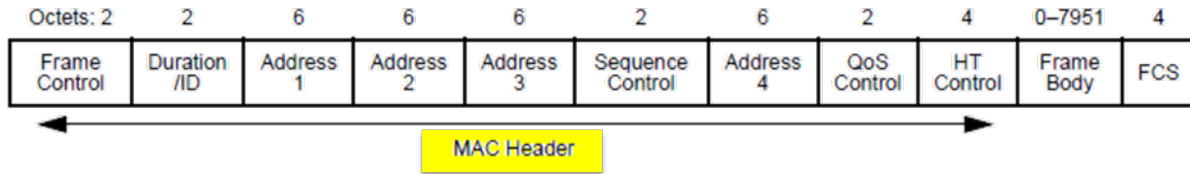


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.
...		
...		
...		
Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

Alternatively, *Orava* provides a teaching of the server controlling an AP. Specifically, *Orava* discloses that the **server** assigns MAC addresses to the **APs**. EX1005, ¶[54] (“In a **server** of the network, for example in the [] **PAC**, a list can be maintained to which the temporary MAC addresses allocated by the different access points **AP** are added. Thus, the **AP** can *transmit a request for allocation* of a temporary MAC address. On the *basis of the request*, the **server** *selects an available address and transmits a response message* comprising the allocated address

MAC.”). This address assignment demonstrates that the server controls the AP. Bims, ¶¶330-375.

Vardi, like *Orava*, discloses a multi-AP system, “radio access points 370a-d,” enabling connections between mobile devices, APs, and the Internet. A POSITA would have found it obvious to add *Orava*’s central server management capabilities, controlling the APs, to *Vardi*’s server because a POSITA would have understood the need to manage and distribute access point configurations within the system, for example, utilizing a single “SSID” for the “access points 370a-d.” Bims, ¶¶330-375. Additionally, *Orava* assures that the randomly generated Fake IDs will be unique across APs by allocating specific MAC address space per AP. EX1005, ¶[54] (“In a server of the network... a list can be maintained to which temporary MAC address allocated by the different [] AP are added... the server selects an available address and transmits a response...”).

Section IV.A.6.a *supra* further explains that a POSITA would have found it obvious to combine the teachings of *Vardi*, *IEEE802.11*, *Orava*, and *Yun* because their teachings align and *Vardi*, *Orava*, and *Yun* are all built upon *IEEE802.11*. Bims, ¶¶88-123.

- c. 10[b]: “receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;”

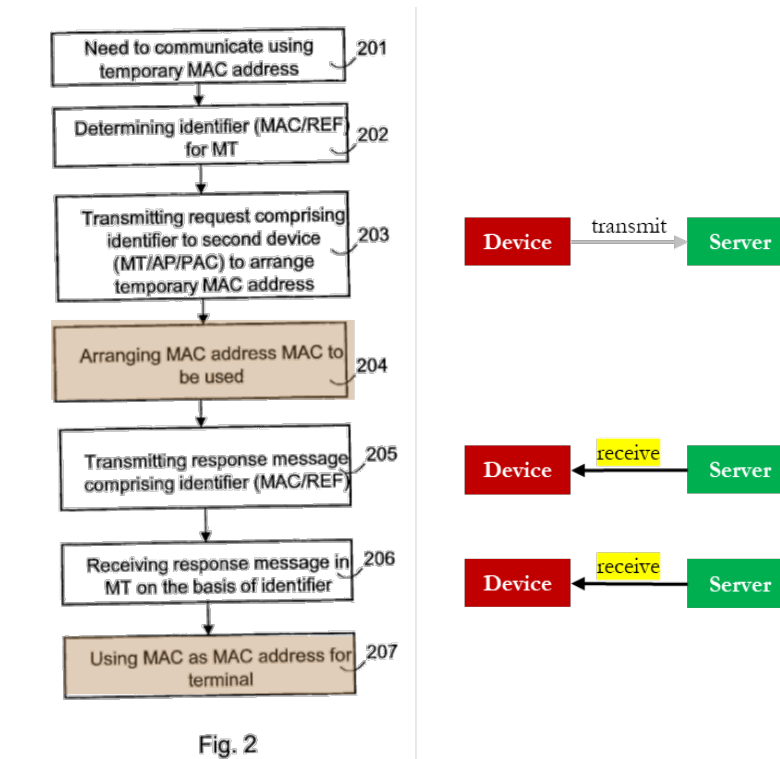
Vardi-IEEE802.11-Orava-Yun render obvious this limitation. Bims, ¶¶376-403.

The mobile device receives a randomly generated Fake ID from the server. *Orava* discloses a **mobile device** generating a REF identifier and transmitting the REF identifier to a centralized **server—public access controller PAC**—to arrange for a **temporary MAC address MAC**⁶ (“Fake ID”). EX1005, ¶[26] (“The **second device** transmits a response message relating to the arrangement of the **MAC address** comprising an identifier (MAC/REF)... the **second device** may be. . . a **public access controller PAC**... the **second device** allocates a **temporary MAC address MAC** on the basis of the request.”); ¶¶[32], [34], FIG. 2.

The server randomly generates the Fake ID to falsely identify the device for use in a probe request frame. *Orava* discloses “**MAC**” can be generated utilizing a random number generator, selection algorithm, specific organization unique identifiers, or formed of a network identifier, such as a BSS identifier BSSID,

⁶ Orava refers to “MAC” for the generated temporary random MAC address; to avoid confusion, Samsung refers to it as **Fake ID**.

and a random part added. *Orava*'s server generates the **Fake ID** in IEEE MAC address format, which is used to falsely identify the device in *Vardi*'s probe request frame. EX1005, ¶[30] ("IEEE 802 MAC address format allows locally administrable MAC addresses... for selecting the **temporary MAC address**."); FIGS. 3-4.



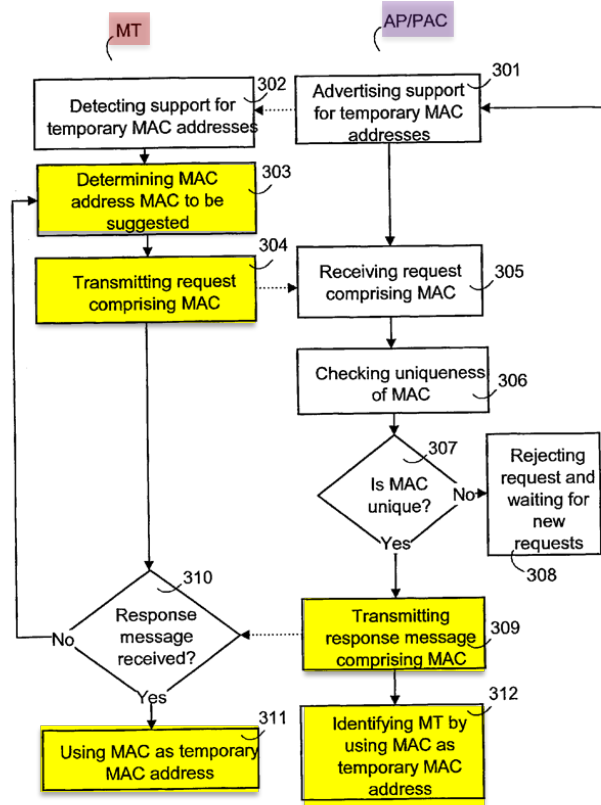
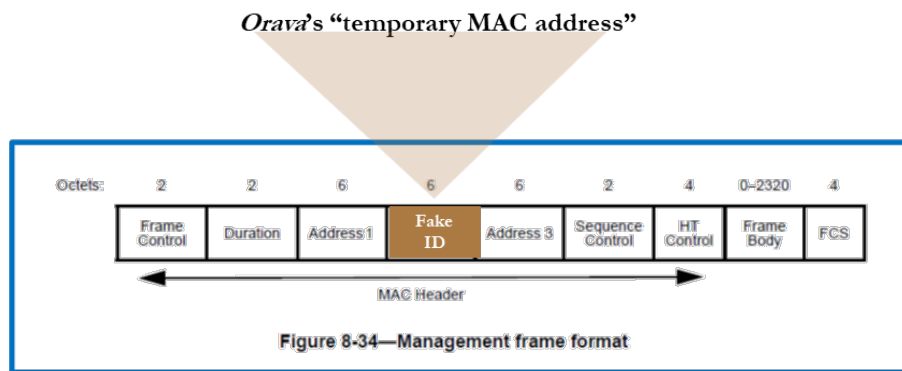
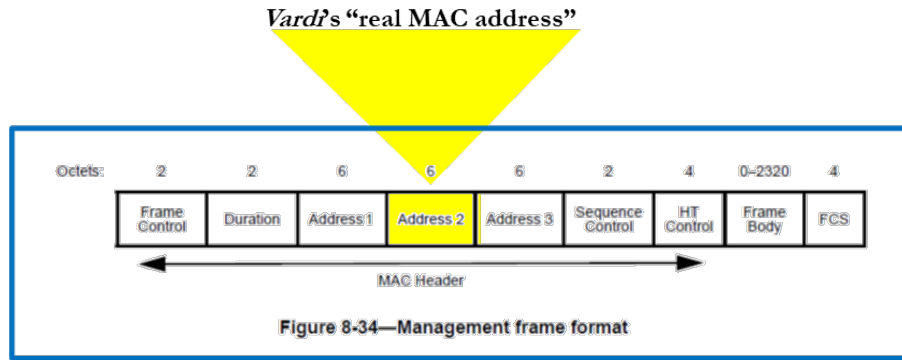


Fig. 3

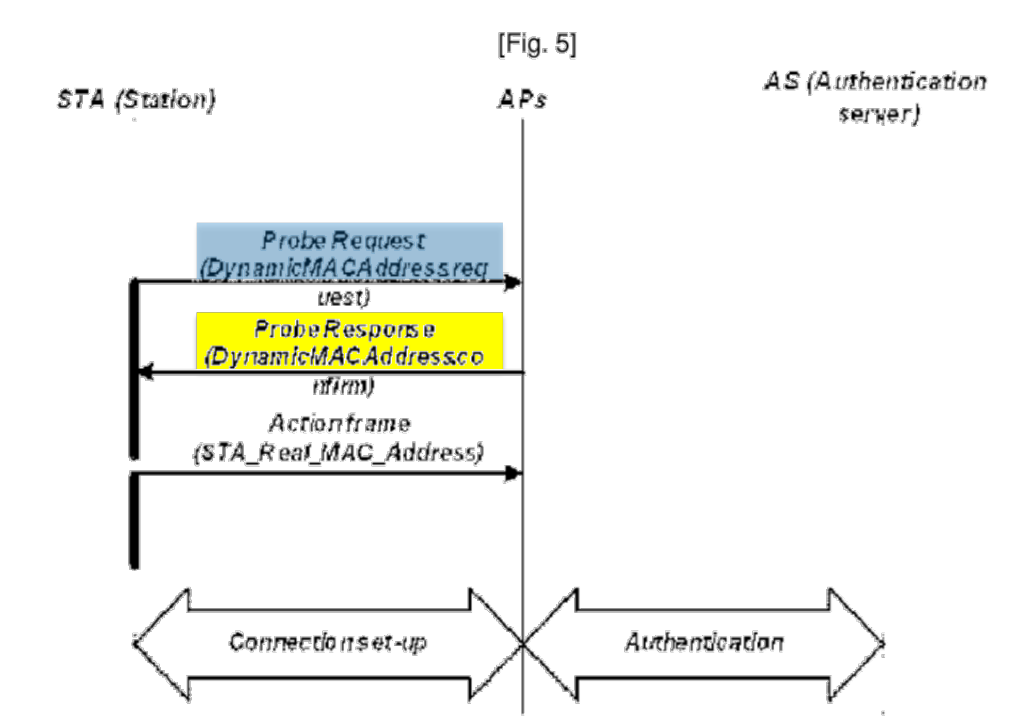
It would have been obvious to a POSITA to apply the randomly generated MAC address to *Vardi's* probing message as defined by *IEEE802.11*. *Orava* explicitly informs a POSITA that “**MAC**” follows the IEEE MAC address format, IEEE802.11 “allows locally administrable MAC addresses,” and that “[p]referably, the use of a *temporary MAC address MAC does not, after arrangement of the address, differ in any way from the use of a fixed MAC address* permanently allocated by the manufacturer. The *temporary MAC address can thus be used instead of a fixed address in all protocol messages.*” EX1005, ¶[30]; Bims, ¶¶376-403.



But even assuming that *Vardi* and *Orava* do not teach or at least render obvious using the Fake ID to “*falsely identify the device in a probe request frame*”—which it does—*Vardi* in view of *Orava* and *Yun* explicitly directs a POSITA to using the received generated Fake ID in a “probe request” to have “MAC address anonymity[, which] makes an identity of the station(12) not presumed through the MAC address.” EX1004, ¶[154], FIG.5; Bims, ¶¶376-403. *Yun* is explicit teaching that “the station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).” Where *Yun* explains that “the transmitted packet on air uses an arbitrary MAC address (‘Dynamic MAC address’) which is dynamically allocated.” EX1004, ¶¶[154-156]. Thus, a POSITA would have found it obvious to combine *Vardi*,

Orava, and *Yun* to transmit the received MAC address (*Orava*) in the probe request message (Vardi/IEEE802.11). Bims, ¶¶376-403.

Section IV.A.6.a explains, *Vardi*, *Orava*, and *Yun* utilize IEEE802.11 probe request/response messages to communicate with APs. *Orava*'s **Fake ID** is formatted as an IEEE802 MAC address and, thus, only requires exchanging one set of characters for another set explaining that the **Fake ID** can be used the same as the fixed MAC address in “*all protocol messages*.” EX1005, ¶[49]; Bims, ¶¶376-403. While *Yun* explicitly discloses transmitting the **Fake ID** in the **probe request message**. See FIG.5, ¶¶[154-156]; Bims, ¶¶88-123, 37-57.



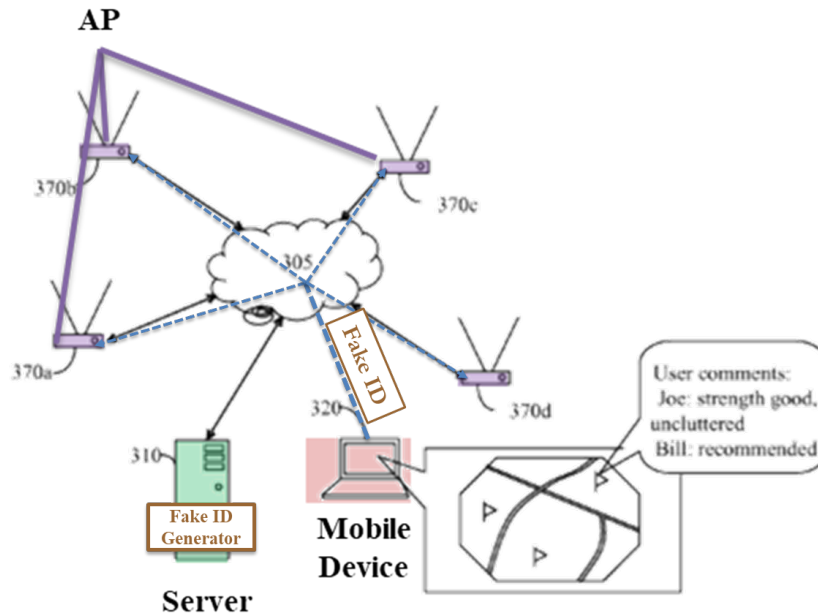


Figure 3

- d. 10[c]: “transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;”

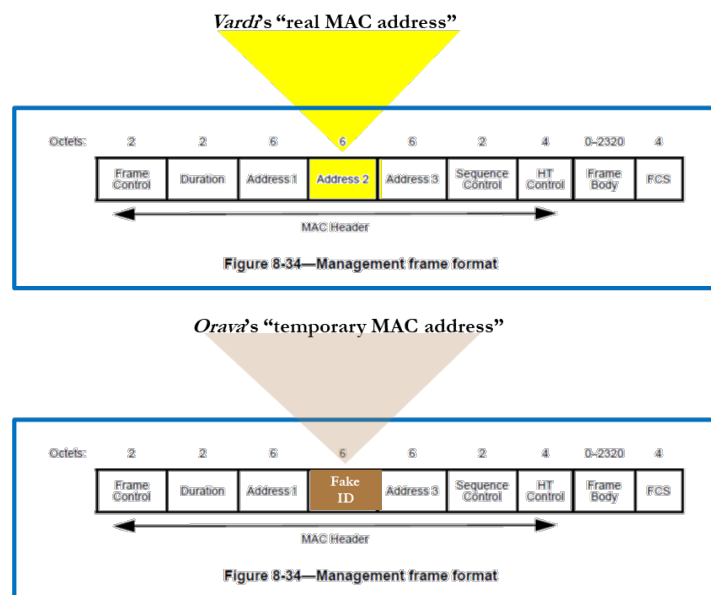
Vardi-IEEE802.11-Orava-Yun render obvious this limitation. Bims, ¶¶404-411.

The mobile device transmits a probe request—including the Fake ID—to the AP. As explained in limitations 10[a-b], *Vardi-IEEE802.11-Orava-Yun* render obvious the **mobile device** transmitting a **probe request** including the **Fake ID** to an **AP**. See limitation 10[b]; Bims, ¶¶404-411. As explained above, in the combined system, *Vardi*’s mobile device receives a generated random Fake ID from the server,

then the mobile device transmits the received randomly generated Fake ID in a probe request to the AP. See limitation 10[b].

Particularly, *Yun* discloses the “*transmitted packet on air uses an arbitrary MAC address* (‘Dynamic MAC address’)” to provide “MAC address anonymity.” Specifically, *Yun* teaches that the “*station(12) transmits the data* including the *MAC address request such as the probe request*(‘Dynamic MAC address request’) to the *access points(14)*.” EX1004, ¶¶[154-156]; Bims, ¶¶404-411.

Indeed, it would also be obvious to a POSITA to substitute *Vardi*’s “real” MAC address with *Orava*’s received Fake ID in *Vardi-IEEE802.11*’s probe request frame (as illustrated below). Again, *Orava* disclosed the purported problem the ’552 patent attempted to solve. As *Orava* recognized, “[i]n order to arrange anonymity, it has been suggested that temporary random MAC addresses be used for WLAN networks.” ¶[4].



And to the extent the PO contends that *Vardi*, *Orava*, and *Yun* do not explain how a POSITA transmits the Fake ID in a probe request message—neither does the ’552 patent—*IEEE802.11* provides the underlying implementation details. *Vardi*, *Orava*, and *Yun* presume a working knowledge of *IEEE802.11*—like the ’552 patent—and thus, recognized that a POSITA would understand the workings of “probing,” and transmitting a frame within a “probe message.” Regardless of whether the POSITA possessed that working knowledge, *Vardi*, *Orava*, and *Yun* direct a POSITA to look to *IEEE802.11* for those details.

Specifically, *IEEE802.11* defines the implementation details underpinning *Vardi*, *Orava*, and *Yun*. As identified below and in Section VII.A.1.g *infra*, the *IEEE802.11* probe request frame includes transmitting a MAC address—(e.g., Address 2)—within the probe request sent by the device to the AP. Bims, ¶¶404-411; EX1009, FIGS. 4-17 (“Establishing the IEEE 802.11 association”), 8-34; 10-3.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

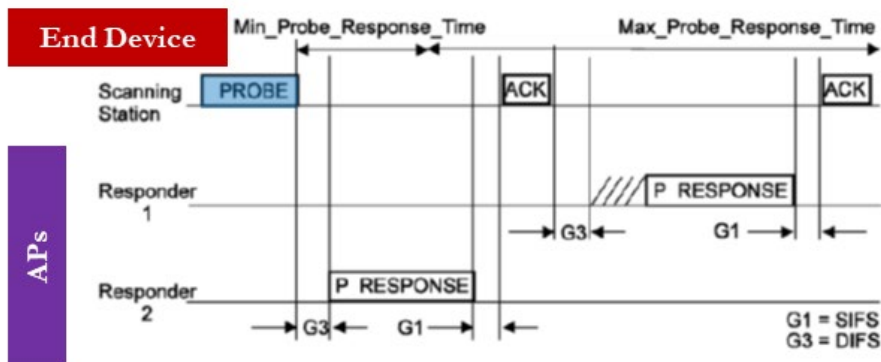


Figure 10-3—Probe response

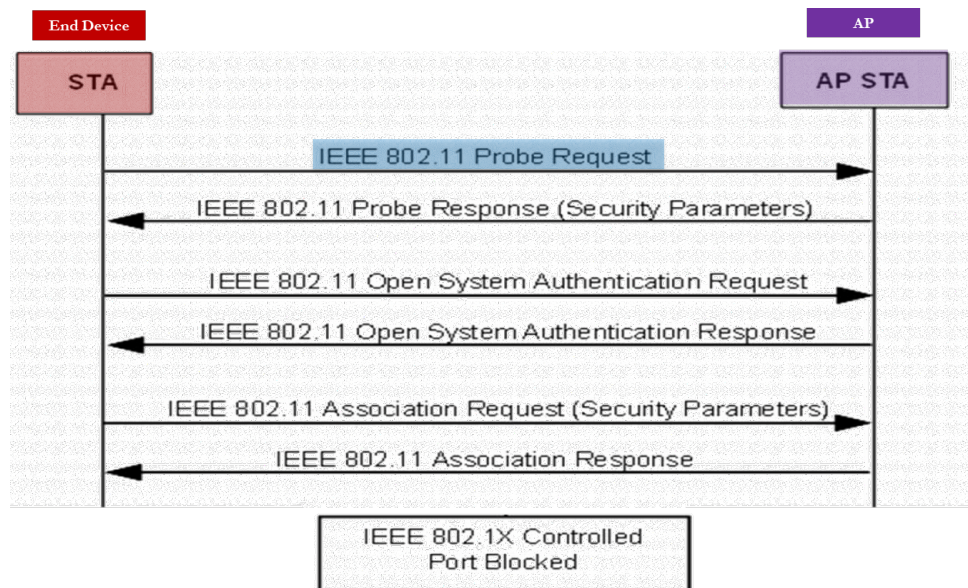


Figure 4-17—Establishing the IEEE 802.11 association

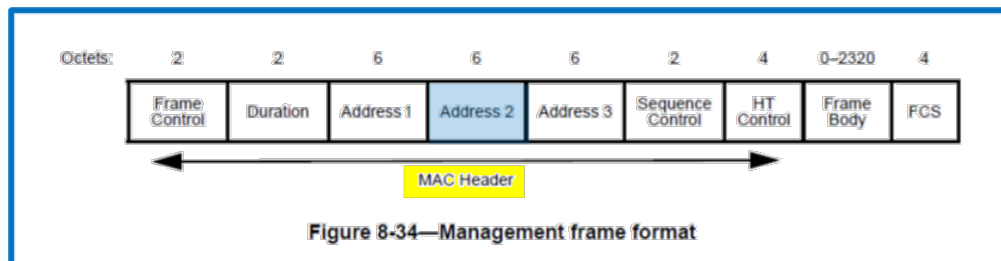


Figure 8-34—Management frame format

The address fields for all management frames except Multihop Action frames are as follows:

- The Address 1 field of the management frame is the RA (=DA) and is determined as the destination of the frame.
- The Address 2 field of the management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame.
- The Address 3 field of the management frame is set and determined as follows:
 - In management frames of subtype Probe Request, the Address 3 field is the BSSID. The BSSID is either a specific BSSID as described in item 4) below or the wildcard BSSID as defined in the procedures specified in 10.1.4.
 - In management frames of subtype Action, Category Public, the Address 3 field is the BSSID. The BSSID value is set according to 10.19.
 - If dot11OCBAActivated is true, the Address 3 field is the wildcard BSSID.
 - Otherwise:
 - If the STA is contained within an AP or is associated with an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - If the STA is contained within an AP or is transmitting the management frame to an AP, the Address 3 field is the BSSID. The BSSID is the address currently in use by the STA contained in the AP.
 - If the STA is transmitting the management frame to one or more members of an IBSS, the Address 3 field is the BSSID of the IBSS.
 - If the STA is a mesh STA, the Address 3 field is the TA.

It would have been obvious to a POSITA at the time of the alleged invention to transmit *Orava*'s received Fake ID as part of *Vardi*'s probing message from the mobile device to the AP as *Orava* explains that the Fake ID can be used the same as the fixed MAC address in “*all protocol messages*,” however, *Yun* removes any doubt that the probe request is included in “*all protocol messages*” by explicitly instructing a POSITA to transmits the received Fake ID in a “probe request(‘Dynamic MAC address request’) to the access points(14).” Bims, ¶¶88-123.

A decade before the '552 patent, *Orava* informed a POSITA that “fixed MAC address determined by manufacturers cause a security risk: a MAC address can be picked up from every message over the air interface...” EX1005, ¶[3]. *Orava* explains, “[i]n order to arrange anonymity, it has been suggested that temporary MAC addresses be used for WLAN networks.” EX1005, ¶¶[4], [27] (“FIG. 2 allows temporary MAC addresses to be arranged reliably and the user to be provided with anonymity...”). *Yun*, like *Orava*, informed a POSITA that it wants to “protect a MAC address” and “MAC address anonymity makes an identity of the station(12) not presumed through the MAC address.” EX1004, ¶[154]. Thus, *Yun*'s disclosure further emphasizes that a POSITA would have found it obvious and been successful transmitting a probe request including a Fake ID.

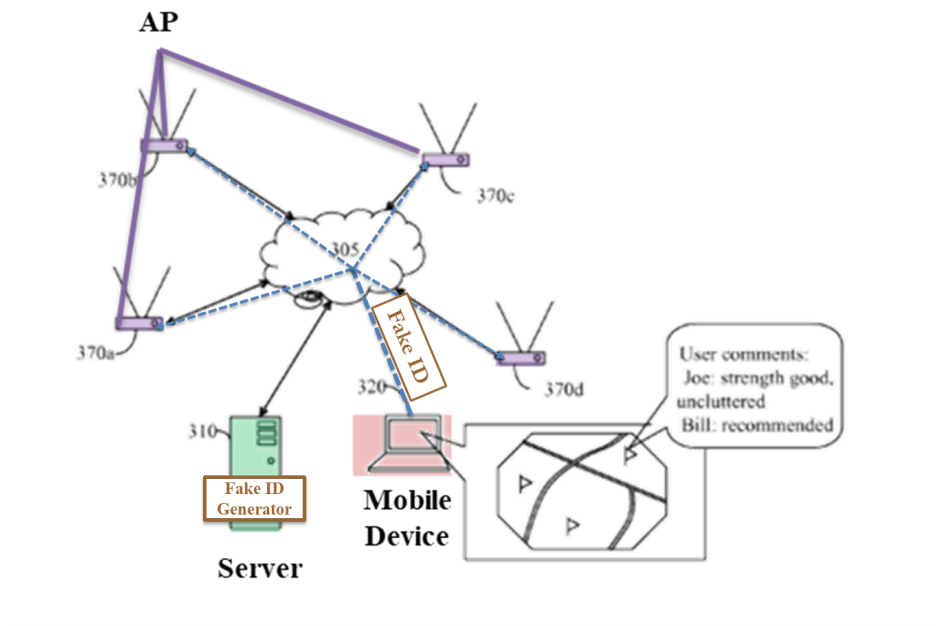
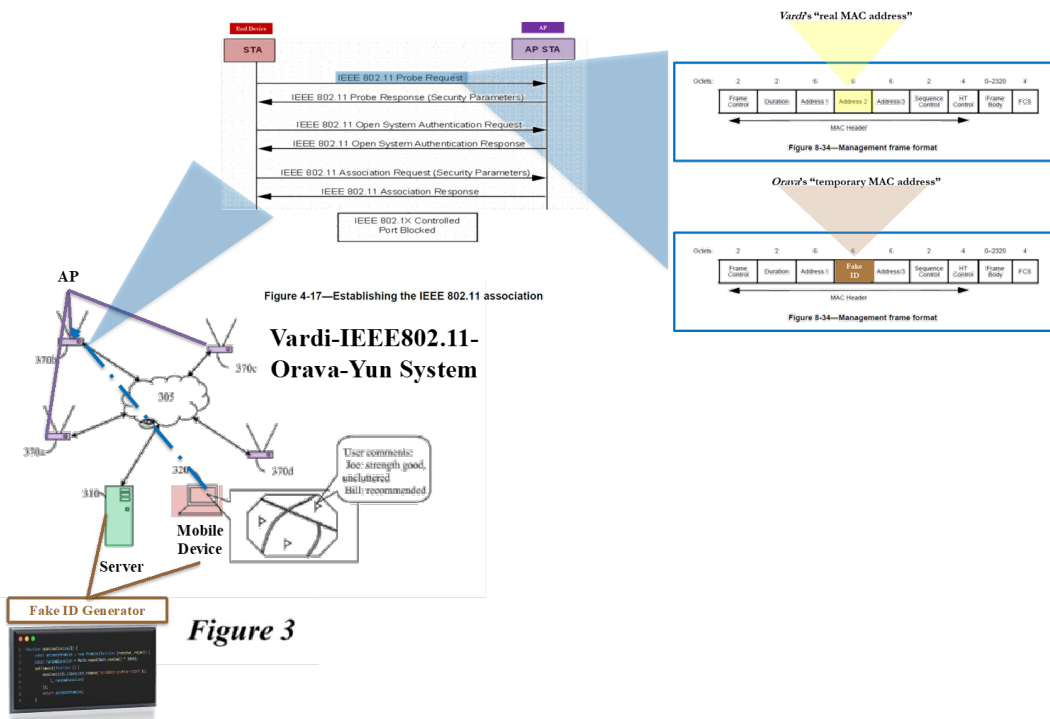


Figure 3



- e. 10[d]: “receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;”

Vardi-IEEE802.11-Orava-Yun render obvious this limitation. Bims ¶¶412-

413. *Vardi-IEEE802.11-Orava-Yun*’s **mobile device** receives, in response to its **probe request**, a **probe response** from **APs** nearby, including **API—SSID** and **MAC Address** of the **AP**.

Vardi explains that the **mobile device** performs a “Basis IEEE 802.11 association procedure... using... probing to get association information” and “information acquired as part of the standard 802.11 scan, i.e.[,]: Network or AP name (SSID—service set identifier); and, AP Radio Mac address” is included in the response from the **AP**. 10:25-36; 13:4-7 (“Connecting to a wireless network starts by scanning the neighborhood for candidate **AP** connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of **access points** in reach.”); 14:52-57 (“When **client** becomes active it executes an IEEE 802.11 scan for **APs** in reach and determines the **SSID, MAC address...**”); 7:10-46; 9:54-64; Bims, ¶¶412-413.

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

As illustrated above, *Vardi* teaches additional information received within the probe response. EX1007, 3:25-54; Bims, ¶¶412-413. Limitation 10[c] *supra* explains that a POSITA would have readily understood at the time of the alleged invention that IEEE802.11 active scan encompass the probe request and response communication between the device and APs. See limitation 10[c]; Bims, ¶¶88-123, 37-57.

But to the extent PO contends *Vardi* does not explicitly disclose the “probe response frame,” *IEEE802.11* defines the communication and frame (illustrated below). *IEEE802.11* explains that APs receiving a probe request frame will respond by issuing a probe response frame. EX1009, 978-980; EX1011, 38-42 (contending the same). The probe response frame includes the AP’s SSID and MAC Address.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

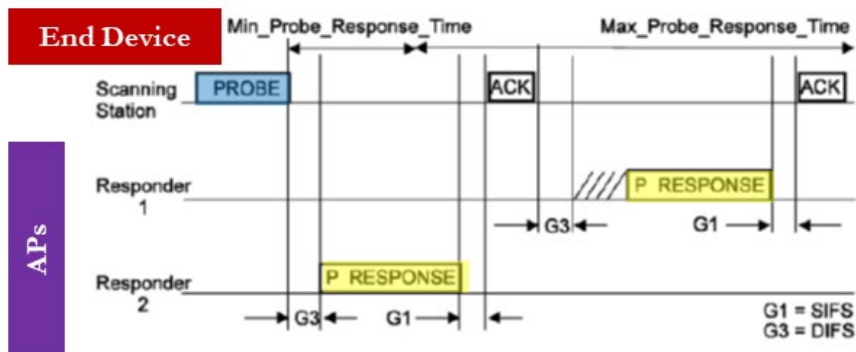


Figure 10-3—Probe response

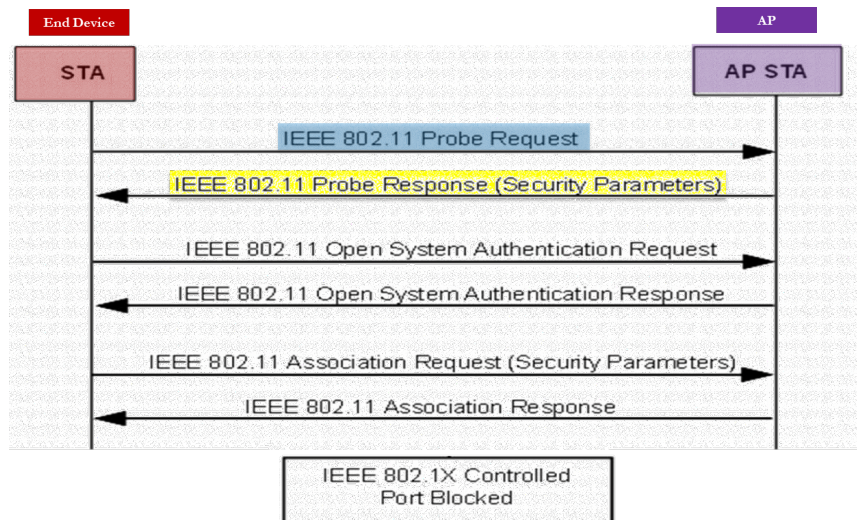


Figure 4-17—Establishing the IEEE 802.11 association

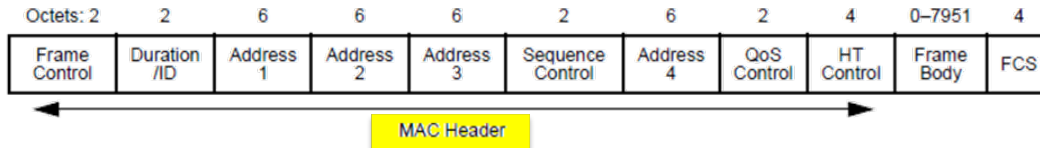


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.
⋮		
⋮		
Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

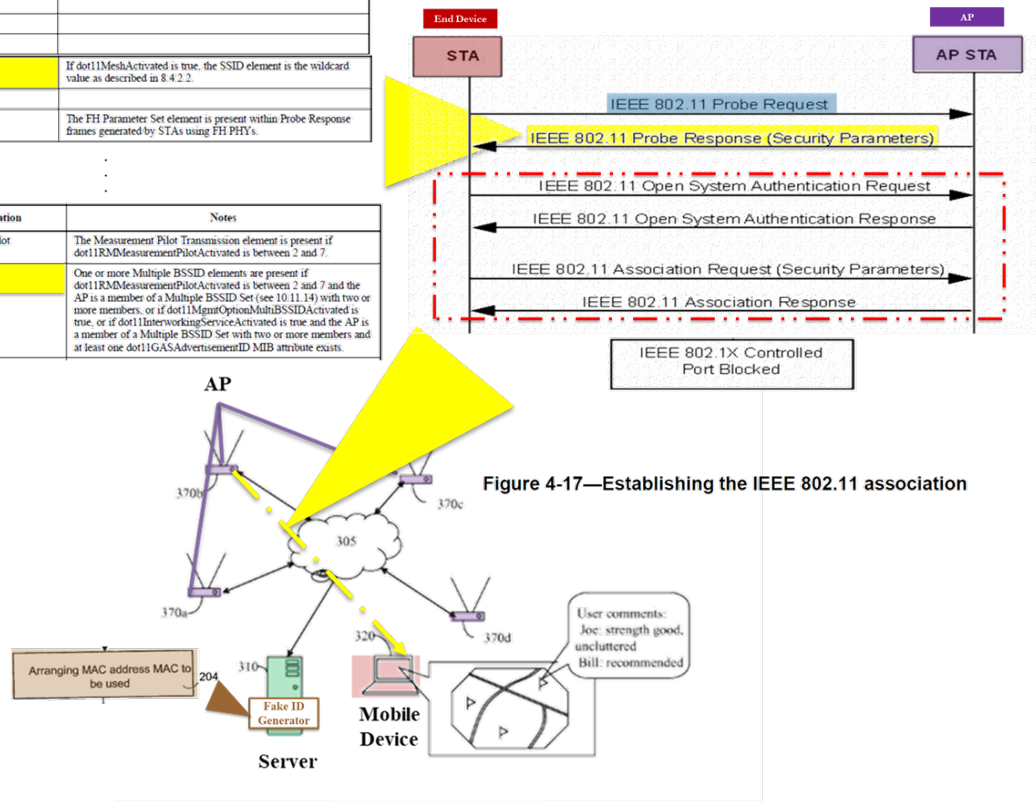


Figure 4-17—Establishing the IEEE 802.11 association

Figure 3

As Section IV.A.6.a explains, a POSITA would have readily looked to *IEEE802.11* to provide the implementation details regarding *Vardi*'s "IEEE 802.11 scan," and "probing." The POSITA would have a likelihood of success applying the implementation details to the *Vardi* system. Bims, ¶¶88-123.

- f. 10[e]: "determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated

access point⁷, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and”

Vardi-IEEE802.11-Orava-Yun teaches this also. Bims, ¶¶414-447.

Vardi discloses that **mobile devices** store **API** received from the **server** in its memory, compare the stored **API** with the **API** received from an IEEE802.11 scan to determine whether the **AP** is the preferred **AP**—the preferred AP being an authenticated access point⁸—and automatically reconnect to that **AP** when the **mobile device** determines that the SSID or MAC address from the IEEE802.11 scan matches that of the received **authenticated access point list** stored in memory. *See* limitations 10[a], 10[d]; EX1007, 14:52-57 (“When **client** becomes active it executes an IEEE 802.11 scan for **APs** in reach and determines the **SSID, MAC address...** Using the **MAC address**, the **client** can compare this scan result with its radio

⁷ Petitioner reserves the right to argue in an appropriate forum that certain limitations in the challenged claims are indefinite.

⁸ For purposes of this proceeding, Petitioner adopts PO’s infringement theory of “authenticated access point” being an access point that the mobile device previously connected with.

resources database [the claimed “authenticated access point list” in memory] to determine which APs are *preferred for connection*...”); Bims, ¶¶414-447.

Further, *Vardi* explains that “it was well known in prior art computing systems” for the devices to store API of previously connected APs facilitating devices to “automatically reconnect to that AP. The cache [memory] normally includes the name and the MAC address of the AP.” EX1007, 12:24-30; Bims ¶¶414-447.

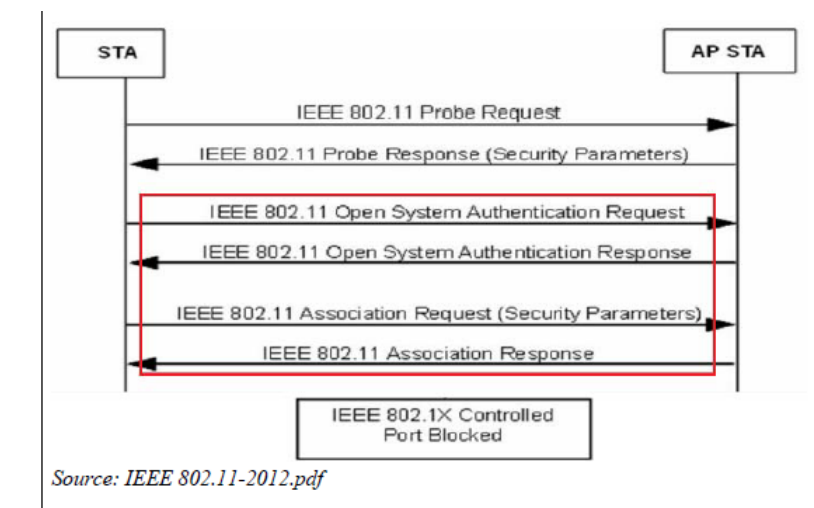
- g. 10[f]: “*transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.*”

Vardi-IEEE802.11-Orava-Yun render obvious this limitation. Bims, ¶¶448-477. *Vardi* discloses the device connecting to the preferred AP after determining the AP is the preferred AP. As explained in the “determining” limitation, *Vardi* discloses that mobile devices store API received from the server in its memory, compare the stored API with the API received from an “IEEE802.11 scan” to determine whether the AP is the preferred AP—the preferred AP being an authenticated access point—and automatically reconnect to that AP when the mobile device determines that the SSID or MAC address from the “IEEE802.11 scan” matches that of the received *authenticated access point list* stored in memory. See limitations 10[a], 10[d-e]; EX1007, 14:52-57 (“When client becomes active it

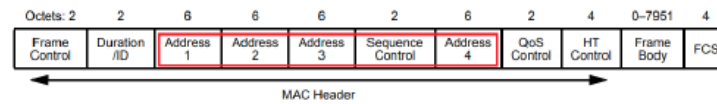
executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resources database [the claimed “authenticated access point list” in memory] to determine which APs are *preferred for connection...*”); Bims, ¶¶448-477.

That is, mobile devices will compare the scan results with the database of access points previously connected to before issuing a connection request to the AP. Bims, ¶¶448-477. As Vardi notes, “the *connection process* (F1 to F5) is being shortened as much as possible depending on whether *radio resource information regarding the target AP is already known.*” 13:36-39, 4-23.

PO’s infringement contentions again cite IEEE802.11 specification as evidence of infringement. Specifically, PO draws a red box around the IEEE802.11 authentication and association steps and cites the “MAC header.”



The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 8-1 depicts the general MAC frame format. The first three fields (Frame Control, Duration/ID, and Address 1) and the last field (FCS) in Figure 8-1 constitute the minimal frame format and are present in all frames, including reserved types and subtypes. The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes. Each field is defined in 8.2.4. The format of each of the individual subtypes of each frame type is defined in 8.3. The components of management frame bodies are defined in 8.4. The formats of management frames of subtype Action are defined in 8.5.



Source: IEEE 802.11-2012.pdf

8.2.4.3.5 DA field

The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field.

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

8.2.4.3.7 RA field

The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

8.2.4.3.8 TA field

The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address.

Source: IEEE 802.11-2012.pdf

EX1011, 59-60 (annotations in original).

Vardi discloses this. The **mobile device**, when “[c]onnecting to a wireless network starts by scanning the neighborhood for candidate **AP** connections (IEEE 802.11 scan)... the connection process will exploit the **radio resource information** in its memory.” 13:4-10. For example, “If a ‘**favorite**’ **AP** (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan ... the **client** can select this **AP** for connection, or If a list of previously successfully used **access points** is available (locally stored) and some **APs** on the list are available ... the **client** can select the **AP** ... for connection.” 13:13-23. Bims, ¶¶448-477, 37-57.

Vardi explains that the mobile device and AP perform an “IEEE 802.11 association procedure” to establish connection. 7:36-40 (“establishing a WiFi connection to the Internet requires a **sequence of steps**, starting with the **IEEE 802.11 association**, continuing with security exchange, essential network IP information acquisition...”), 10:34-35 (“F1—**Basic IEEE 802.11 association procedure (inclusive of WEP, if needed)**”), 50 (“F2—IEEE 802.11 authentications, (WPA, WPA2...)”).

These steps are terms of art that a POSITA would have readily understood because *Vardi*, like the '552 patent, presumes a POSITA has knowledge of *IEEE802.11*. Bims, ¶¶448-477. Particularly, “a POSITA knows that IEEE 802.11 association procedure includes three major steps as defined in *IEEE802.11*: (1) device discovery (“probing”); (2) device authentication (WEP, checking capabilities); and (3) establishing connection (association).” Bims, ¶¶448-477. Thus, a POSITA would have readily understood at the time of the alleged invention that *Vardi* teaches or at least renders obvious transmitting a “connection request” comprising the original MAC address to the AP for connection with the “MAC header.” ¶¶448-477.

However, to the extent PO contends that *Vardi*’s IEEE802.11 association procedure does not explicitly disclose the “authentic device identifier” included in the connection request, *IEEE802.11*’s disclosure does. *IEEE802.11* dictates that a

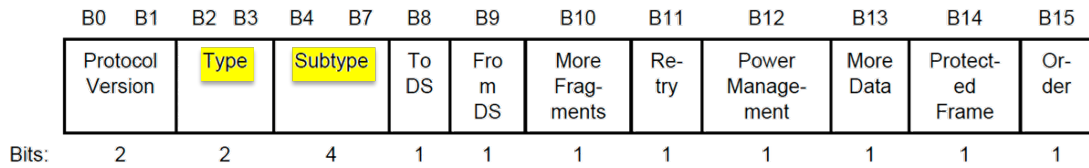


Figure 8-2—Frame Control field

Table 8-1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

After the device discovers and selects the “preferred AP,” it performs an exchange comprising at least four frames (shown in the red dotted box). *IEEE802.11* expressly discloses that the MAC address—authentic device identifier—is transmitted as part of each message Type and SubType for connection. Bims, ¶¶448-477.

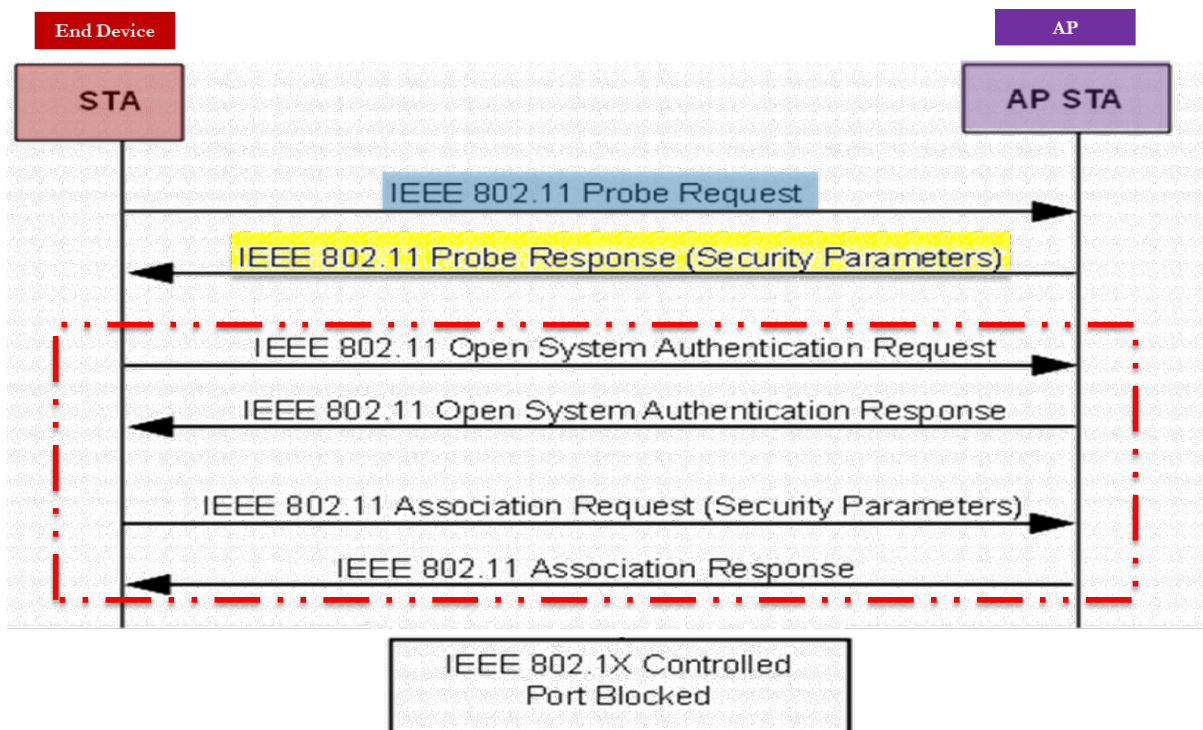


Figure 4-17—Establishing the IEEE 802.11 association

8.2.4.3.5 DA field

The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field.

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

8.2.4.3.7 RA field

The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

8.2.4.3.8 TA field

The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address.

8.2.3 General frame format

The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 8-1 depicts the general MAC frame format. The first three fields (Frame Control, Duration/ID, and Address 1) and the last field (FCS) in Figure 8-1 constitute the minimal frame format and are present in all frames, including reserved types and subtypes. The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes. Each field is defined in 8.2.4. The format of each of the individual subtypes of each frame type is defined in 8.3. The components of management frame bodies are defined in 8.4. The formats of management frames of subtype Action are defined in 8.5.

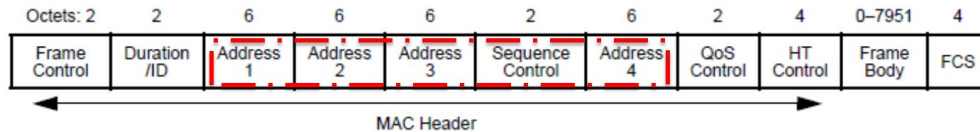


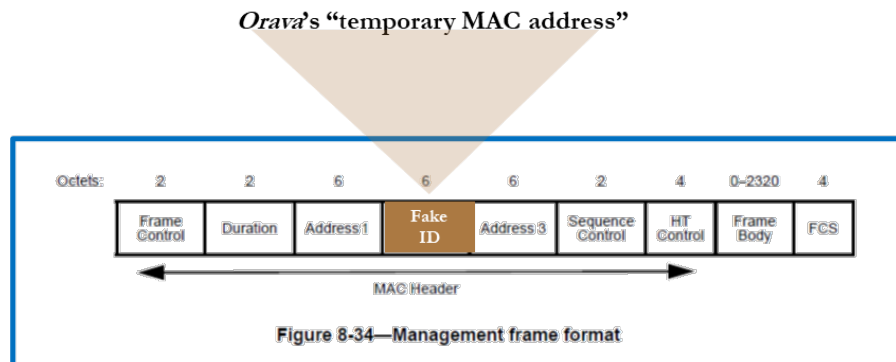
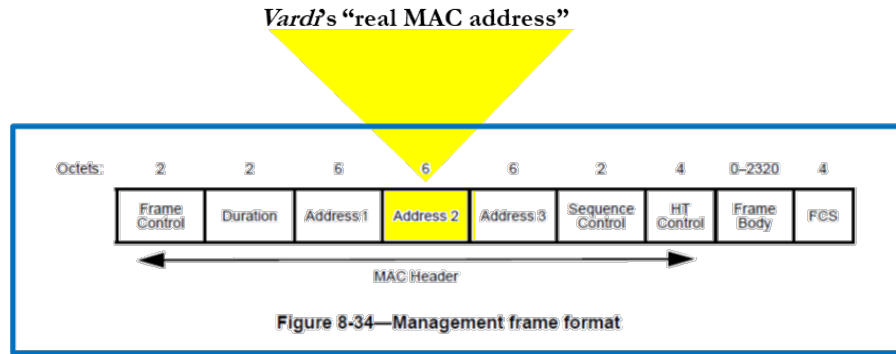
Figure 8-1—MAC frame format

As explained herein, a POSITA would have looked to *IEEE802.11* to implement the necessary components of a connection request. Bims, ¶¶448-477, 88-123, 37-57.

2. Claim 11: “*The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.*”

Vardi-IEEE802.11-Orava-Yun render obvious claim 11. Bims, ¶¶478-483.

Orava discloses that the received “fake device identifier” is in “IEEE 802 MAC address format...in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.” See, limitations 10[b] and 10[c]; EX1005, ¶[30]; Bims, ¶¶478-483.



3. Claim 12: *"The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server."*

Vardi-IEEE802.11-Orava-Yun render obvious claim 12. See limitation 10[a], [e]; Bims, ¶484.

4. Claim 13: *"The method of claim 10, further comprising: storing the authenticated access point list in a memory."*

Vardi-IEEE802.11-Orava-Yun render obvious claim 13. Bims, ¶¶485-492.

As explained above in limitation 10[a], *Vardi* discloses that the mobile device receives API data from the server and stores the received API in its memory. See limitations 10[a] (receiving API from server storing in memory), 10[e] (comparing received API with stored API to determine preferred AP); see also EX1007, 7:23-

32 (“The **information** gathered can provide access point **connection or connectivity data** that can be used by a **wireless user terminal** to connect to a *specific access point*... **clients** can *store some or all of this information in the memory* of the **wireless user terminal**.”), 12:24-30 (“it is well known in prior art computing systems to *cache information related to an access point* to which the **mobile device** has connected before... the system uses this **information** in *cache* to automatically reconnect to that **AP**”), 13:13-23 (“If a ‘**favorite**’ **AP** (**AP** is called favorite if it is part of radio resource database that had been distributed to **client**...) is detected by the IEEE 802.11 scan... the **client** can select this **AP** for connection, or If a list of previously successfully used **access points** is available (locally stored) [in memory] and some **APs** on the list are available ... the client can select the **AP** ... for connection”). Bims, ¶¶485-492.

5. Claim 14

- a. 14[a]: “*The method of claim 10, further comprising: receiving, from the at least one access point, an approval of the connection request;*”
- b. 14[b]: “*transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;*”
- c. 14[c]: “*receiving, from the at least one access point, an association response to the association request; and*”
- d. 14[d]: “*connecting to a communication network via the at least one access point in accordance with the association response.*”

Vardi-IEEE802.11-Orava-Yun render obvious claim 14. See limitation 10[f]; Bims, ¶¶494-505. *Vardi-IEEE802.11-Orava-Yun* discloses a mobile device connecting with the preferred AP via IEEE802.11 authentication-association protocol. EX1007, 4:42-48 (searching for and connecting to AP), 7:10-20 (“**wireless user terminal** can be a device that executes a program (e.g., client) that uses the combined data to find usable **radio resources or wireless APs** and **establish network connections** through them, for example, connections to the internet.”), 7:36-43 (“establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition and accessing specific network location.”).

To the extent PO contends that *Vardi*’s disclosure connecting the **mobile device** and **AP** via the “IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition” procedure does not explicitly disclose or teach claim 14, *IEEE802.11* does. EX1009, 86, FIG.4-21; Bims, ¶¶494-505. Claim 14 merely recites the steps required by an IEEE 802.11 connection procedure. Bims, ¶495. As shown below, *IEEE802.11* defines the connection procedure between a **mobile device** (“**STA**”) and an **AP** (“**AP STA**”). *IEEE802.11* illustrates that after the **mobile device** and **AP** exchange probe **request** and **response** frames, the **mobile device** transmits an associate request, and the mobile device receives the

AP's transmitted association response, at which point the mobile device and AP are connected to the network via the AP. Bims, ¶¶494-505.

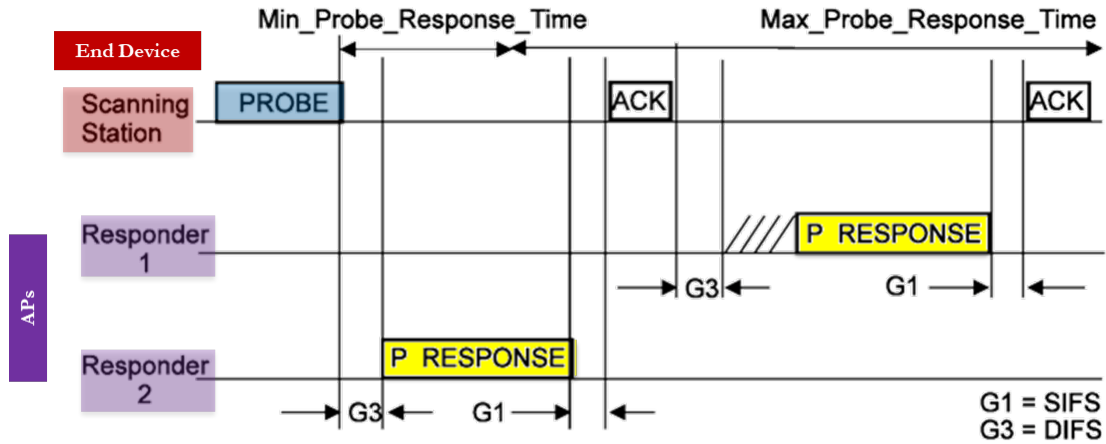


Figure 10-3—Probe response

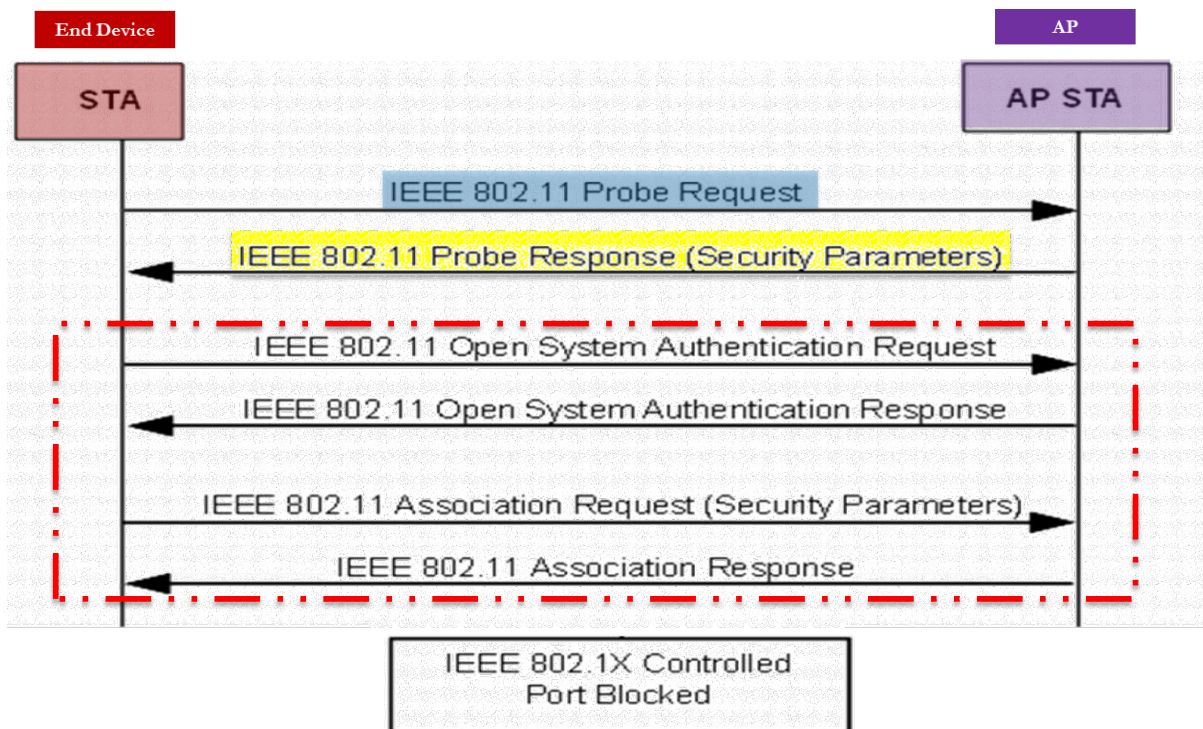
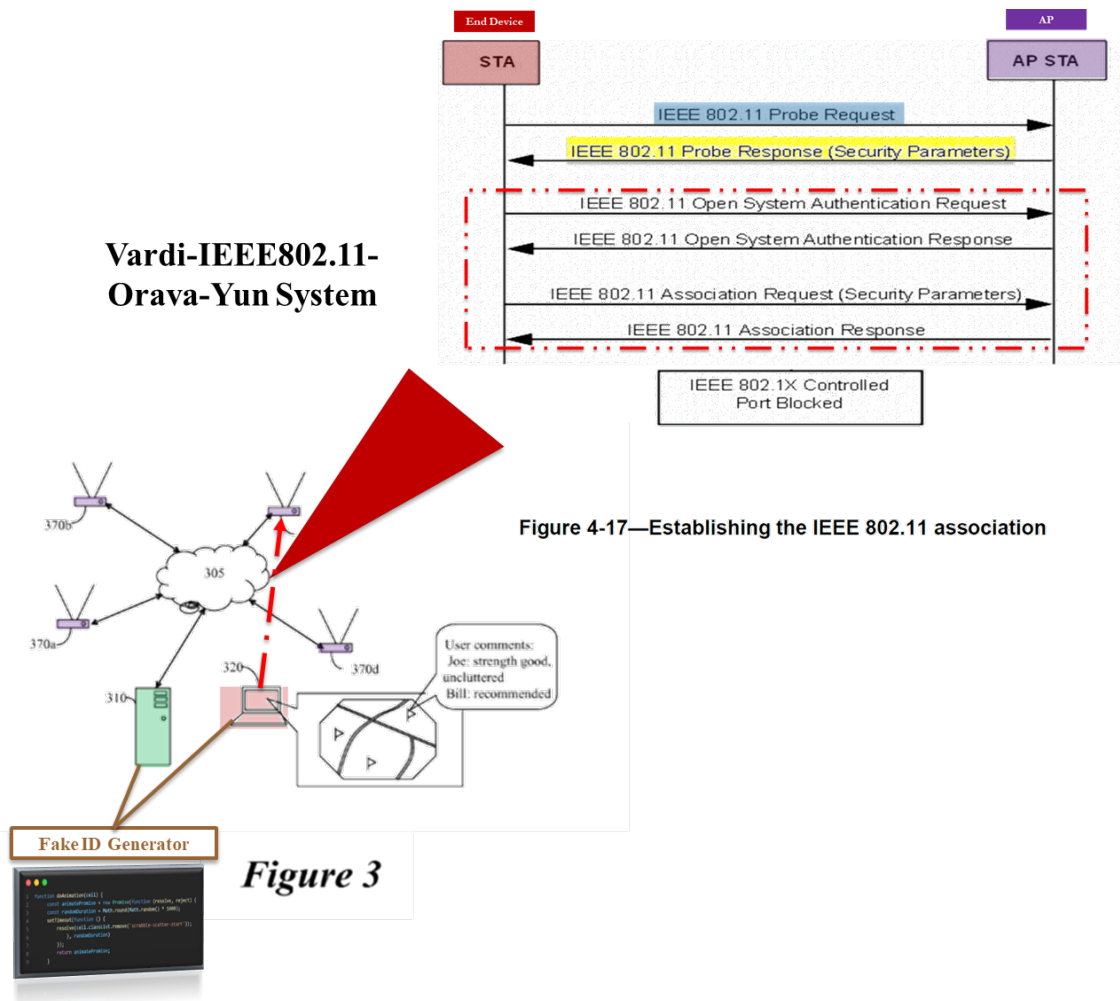


Figure 4-17—Establishing the IEEE 802.11 association

A POSITA would have found it obvious to review the underlying implementation providing by the *IEEE802.11* standard to establish a connection of its mobile device to the network. Bims, ¶¶494-505, 88-123.

Vardi-IEEE802.11- Orava-Yun System



6. Independent Claim 15

- a. 15[pre]: “*A method performed by a device, the method comprising:*”

See, limitation 10[pre].

- b. 15[a]: “*receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;*”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[a]. Bims, ¶508.

See limitation 10[a]; Bims, ¶¶330-375.

- c. 15[b]: “*generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;*”

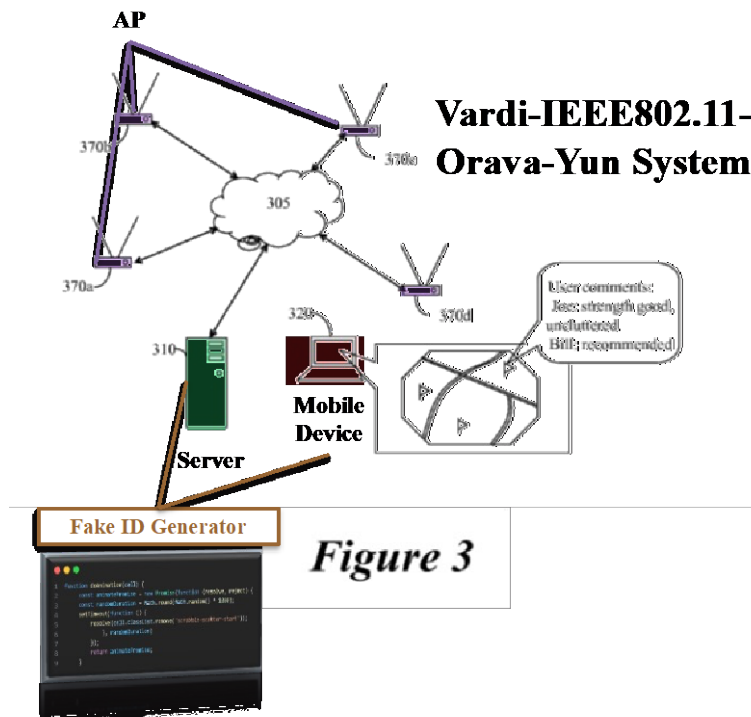
Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[b]. Bims, ¶¶509-522. See, limitation 10[b]; Bims, ¶¶376-403.

Limitation 15[b] differs from limitation 10[b] only in that the Fake ID is generated on-device instead of received, *Orava* also teaches an on-device generation of the Fake ID. *EX1005*, ¶[29] (“When the terminal MT detects that the AP supports the use of temporary MAC addresses, *it determines* the MAC address MAC to be suggested.”) Further, as explained in limitation 10[b], *Orava*’s MAC is generated based upon a selection from one of the numerous algorithms including a random number generator, and the result is an IEEE MAC formatted address. *EX1005*, ¶[30]; limitation 10[b].

A POSITA would not have found a meaningful distinction between executing random generation software, for example, on a server versus mobile device. Bims, ¶511. It would have been obvious to a POSITA to add *Orava*’s on-device randomly generated MAC address capability to *Vardi*’s user terminal. *Orava* explicitly

informs a POSITA that it is advantageous to maintain anonymity when connecting a user device to a WLAN by substituting the real MAC for a randomly generated MAC. EX1005, ¶¶[4], [27]. Both *Vardi* and *Orava* disclose devices implementing IEEE 802.11-compliant MAC addresses.

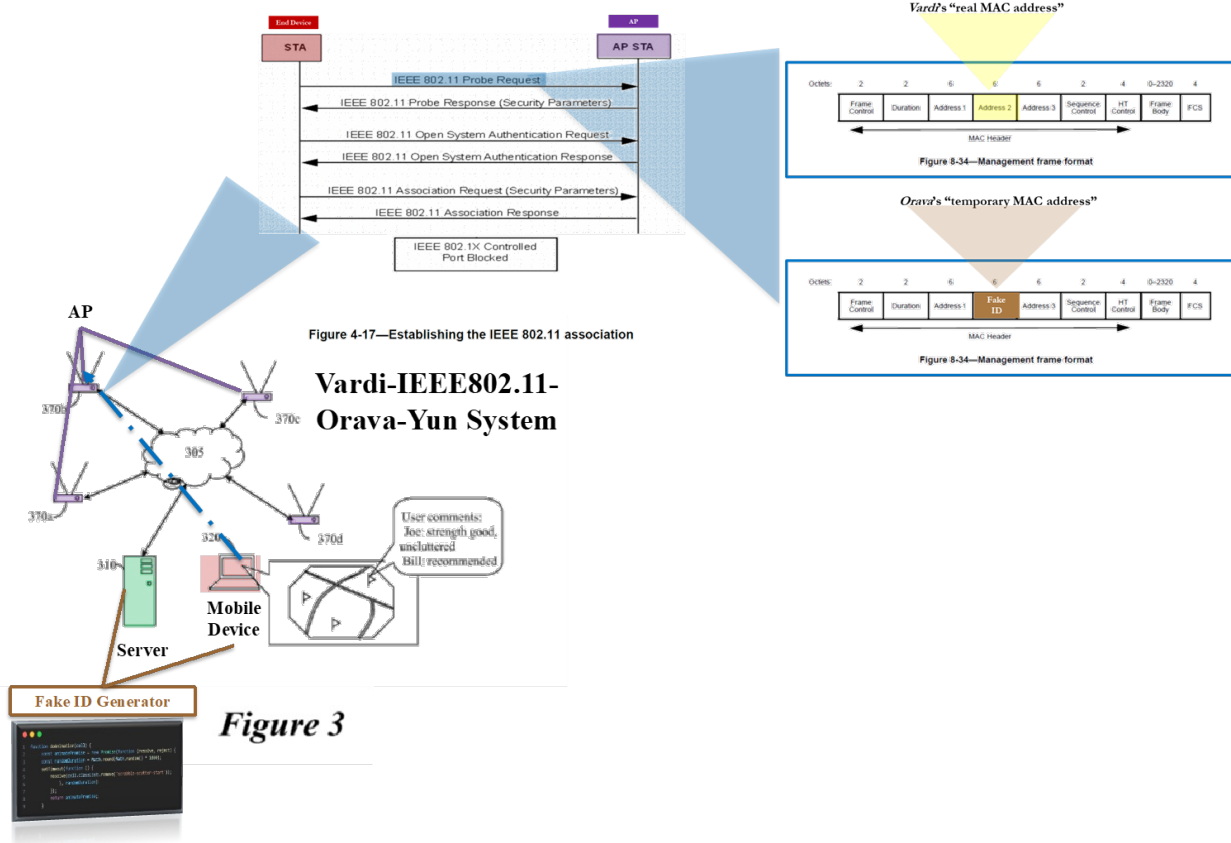
A POSITA would also have had a reasonable expectation of success in doing so because adding software to a mobile device was routine and complying with the IEEE standard would have been typical and expected. Bims, ¶¶88-123.



- d. 15[c]: “*transmitting, to at least one access point, a probe request frame that includes the fake device identifier;*”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[c]. Bims, ¶523.

See, limitation 10[c]; Bims, ¶¶404-411.



- e. 15[d]: “receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[d]. Bims, ¶524.

See, limitation 10[d]; Bims, ¶¶412-413.

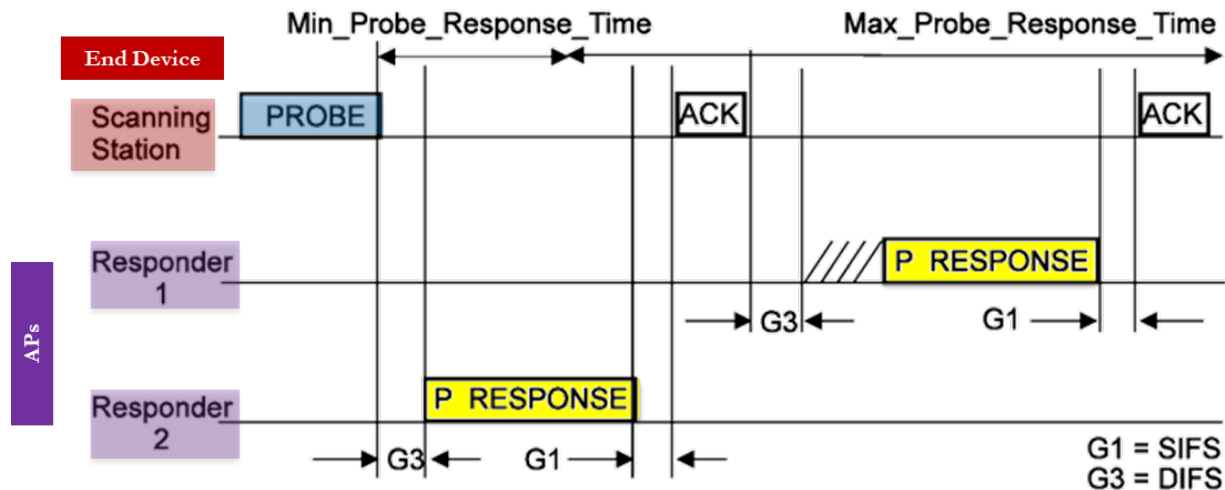


Figure 10-3—Probe response

- f. 15[e]: “determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and”

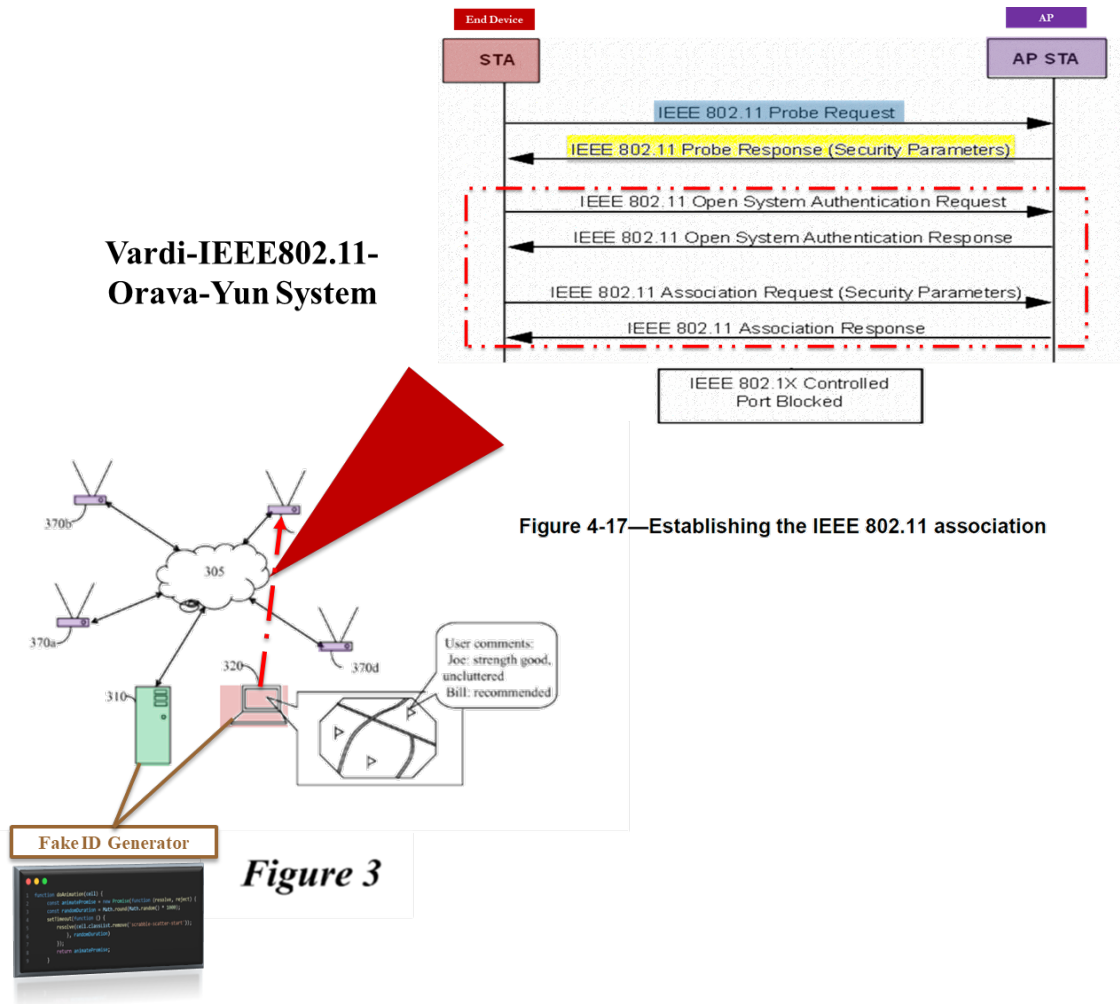
Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[e]. Bims, ¶525.

See, limitation 10[e]; claim 12; Bims, ¶¶414-447, 484.

- g. 15[f]: “transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 15[f]. Bims, ¶526.

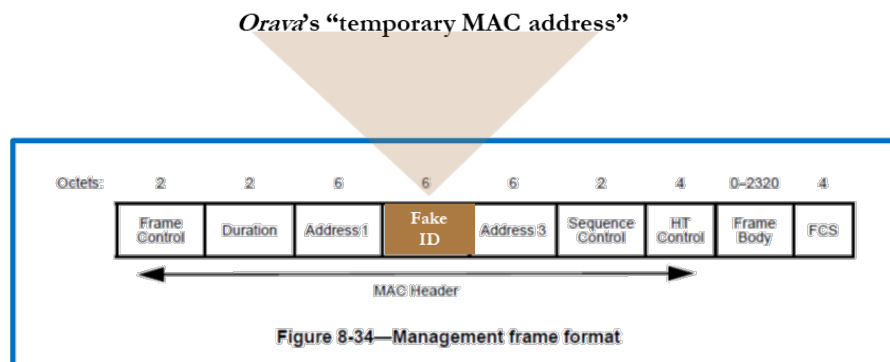
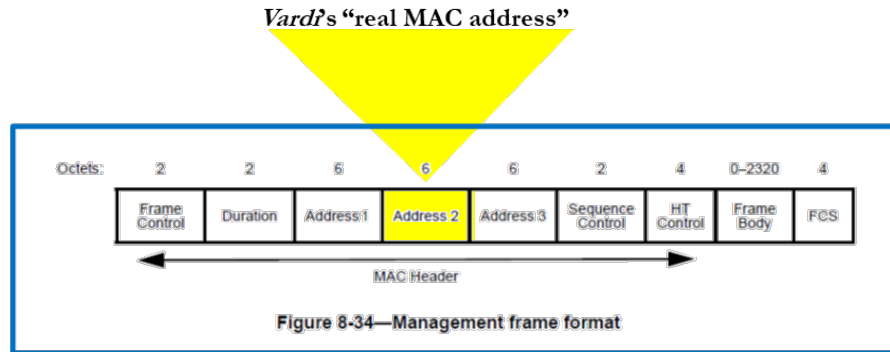
See, limitation 10[f]; Bims, ¶¶448-477.



7. Claim 16: “The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.”

Vardi-IEEE802.11-Orava-Yun render obvious claim 16. Bims, ¶¶527-531.

See, limitation 10[b] and claim 11; Bims, ¶¶527-531.



8. Claim 17: *“The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.”*

Vardi-IEEE802.11-Orava-Yun render obvious claim 17. Bims, ¶¶532-537.

See, limitation 10[b], [c], and claim 11; Bims, ¶¶532-537.

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

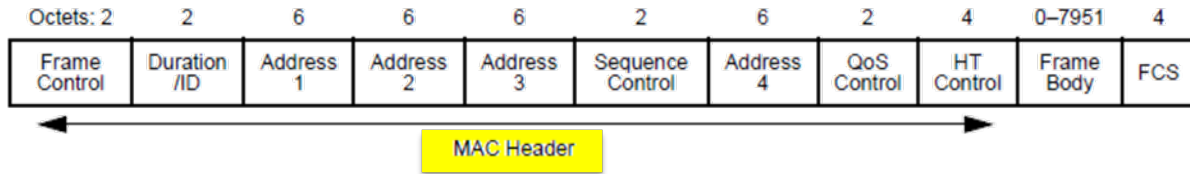


Figure 8-1—MAC frame format

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.
...		
...		
...		
Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

9. Claim 18: “*The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.*”

Vardi-IEEE802.11-Orava-Yun render obvious claim 18. Bims, ¶¶538-542.

See, limitation 10[e] and claim 12; Bims, ¶¶538-542.

10. Claim 19: “*The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.*”

Vardi-IEEE802.11-Orava-Yun render obvious claim 19. Bims, ¶¶543-549.

See, limitation 10[d] and claim 13; Bims, ¶¶543-549.

11. Claim 20

- a. 20[a]: *“The method of claim 15, further comprising: receiving, from the at least one access point, an approval of the connection request;”*
- b. 20[b]: *“transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;”*
- c. 20[c]: *“receiving, from the at least one access point, an association response to the association request; and”*
- d. 20[d]: *“connecting to a communication network via the at least one access point in accordance with the association response.”*

Vardi-IEEE802.11-Orava-Yun render obvious claim 20. Bims, ¶¶551-562.

See claim 14; Bims, ¶¶551-562.

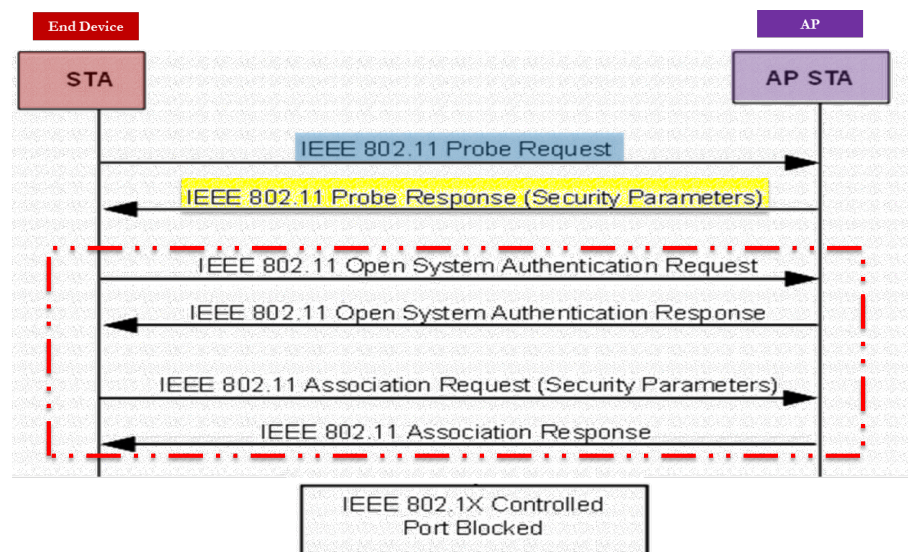


Figure 4-17—Establishing the IEEE 802.11 association

12. Independent Claim 21

Vardi-IEEE802.11-Orava-Yun render obvious claim 21. See claim 10; Bims, ¶563.

- a. 21[pre]: *“A method performed by a device, the method comprising:”*

See, limitation 10[pre]; Bims, ¶¶564-565.

- b. 21[a]: *“receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;”*

Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[a]. Bims, ¶566.
See, limitation 10[a]; Bims, ¶¶330-375.

- c. 21[b]: *“generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;”*

Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[b]. Bims, ¶567.
See, limitations 10[b], 15[b]; Bims, ¶¶376-403.

- d. 21[c]: *“transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;”*

Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[c]. Bims, ¶568.
See, limitation 10[c]; Bims, ¶¶404-411.

- e. 21[d]: *“receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;”*

Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[d]. Bims, ¶569.

See, limitation 10[d]; Bims, ¶¶412-413.

- f. 21[e]: “determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[e]. Bims, ¶570.

See, limitation 10[e]; claim 12; Bims, ¶¶414-447.

- g. 21[f]: “transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.”

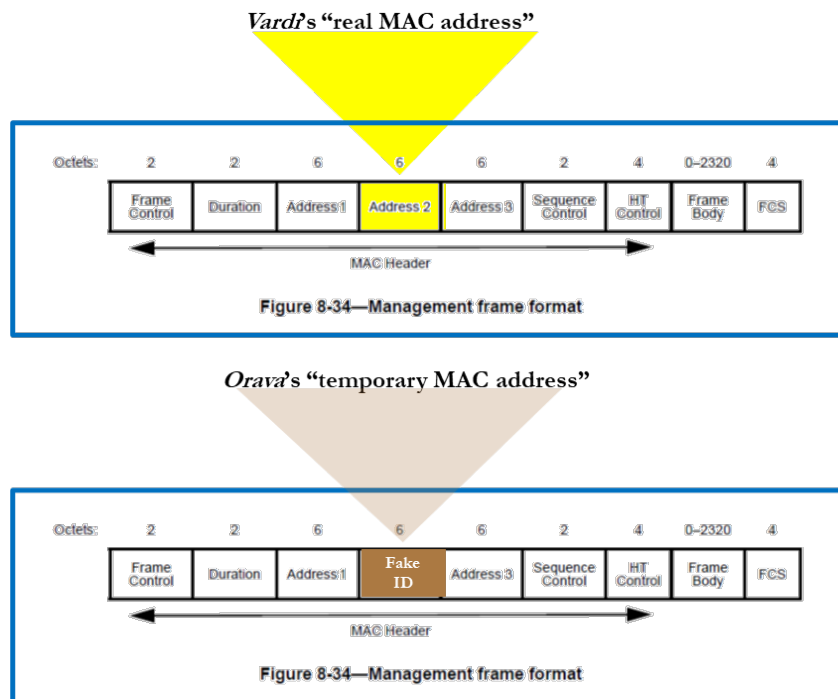
Vardi-IEEE802.11-Orava-Yun render obvious limitation 21[f]. Bims, ¶571.

See, limitation 10[f]; Bims, ¶¶448-47.

- 13. Claim 22: “The method of claim 21, wherein: the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and the fake device identifier includes the fake media access control (MAC) address.”

Vardi-IEEE802.11-Orava-Yun render obvious claim 22. Bims, ¶¶572-578.

As explained above, *Orava* discloses an on-device randomly generated **Fake ID** that is in IEEE MAC address format. See, limitations 10[b], 21[b]; EX1005, ¶[30] (“**MAC** can be a random number generated... IEEE 802 MAC address format... in which there are 46 available bits in a 48-bit address format for selecting the temporary **MAC** address.”)



14. Claim 23: “The method of claim 21, further comprising: storing the fake device identifier in a memory.”

Vardi-IEEE802.11-Orava-Yun render obvious claim 23. Bims, ¶¶579-583.

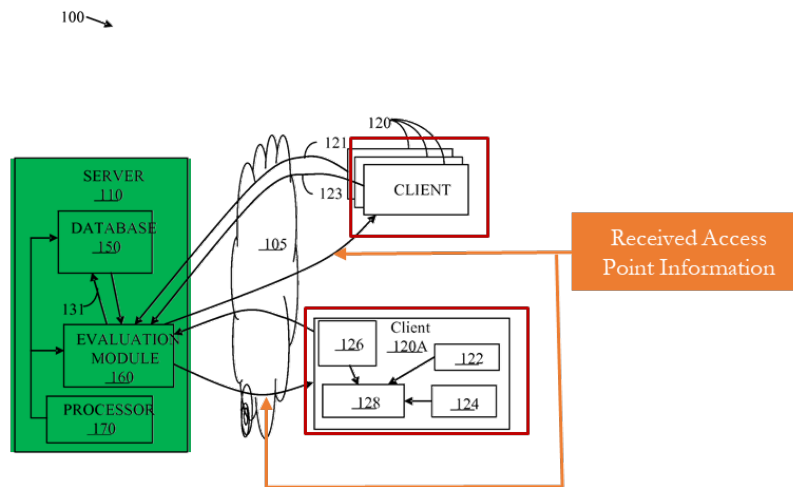
As explained above, *Vardi-IEEE802.11-Orava-Yun* discloses both receiving from a server and an on-device randomly generated MAC address, which the mobile device stores in memory for later use. See, limitations 10[b], 21[b] Bims, ¶¶579-583;

EX1005, ¶¶[70] (e.g., “Each MAC address determines a temporary or *fixed context*.”), [58] (“the terminal MT must request for reconfirmation of the temporary MAC address MAC (indicate in request **304, 405** that it is not new MAC address) if the address has not been used for a long time.”).

15. Independent Claim 24

a. 24[pre]: “*A system, comprising:*”

Vardi discloses a wireless communication system 100 where the **mobile device** performs a method for connecting to the Internet via an **access point** using **access point information** (“**API**”) it received from the **server**. EX1007, 3:11-27; *Id.*, 4:18-27; 4:42-48; FIG. 2.



- b. 24[a]: “*a processor;*”
- c. 24[b]: “*at least one communication interface;*”
- d. 24[c]: “*a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes*

at least one of one or more random numbers or one or more random characters;”

- e. 24[d]: *“a receiver to:”*
- f. 24[d][i]: *“receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and”*
- g. 24[d][ii]: *“receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;”*

Vardi-IEEE802.11-Orava-Yun render obvious limitations 24[a]-[d]. Bims, ¶¶584-597. Limitations 24[a]-[d] add nothing more to claim 10 than well-known mobile device components: (1) processor; (2) communication interface; (3) transmitter; and (4) receiver to perform the method steps of claim 10. Bims, ¶¶584-597. Each of these well-known mobile device components are disclosed by *Vardi*. Bims, ¶¶584-597.

Processor. *Vardi* discloses a “processor” executes a client program for finding usable APs and establishing network connections through them. *Vardi* further explains that the system can employ a client/server architecture where the client is a software program executed on the device. EX1007, 7:10-20; Bims, ¶¶584-597.

Although a POSITA would understand *Vardi* discloses “a processor,” to the extent PO contends the disclosure is not explicit, *Orava* discloses “MT comprises...

a central processing unit CPU comprising one or more processors.” EX1005, ¶[21]; Bims ¶¶584-597.

Communication Interface for transmitting and receiving. *Vardi* discloses “clients continuously collect radio resource information about APs detected by the wireless user terminal... clients can be executed on laptops, handheld devices (PDA’s), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.” EX1007, 9:54-62; FIGs. 1, 3 (depicting mobile device in wireless communication—transmitting and receiving—with a server and APs to connect to the Internet); Bims, ¶¶584-597. Thus, *Vardi* discloses that each of these mobile devices incorporate “a radio facility for wireless communication,” the claimed “communication interface.” As Dr. Bims explains, a POSITA would have readily understood that *Vardi*’s mobile device included the “communication interface” and that “communication interface” performed both transmitting and receiving. EX1007, 3:11-13 (“connecting a wireless user terminal to a network, such as the internet,”), 3:62-63 (the device “transmitting the first set of data to a server over a network or the Internet,”), 5:12-15, 9:54-62, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address...”), 17:61-63, FIGs. 1, 3; Bims, ¶¶584-597.

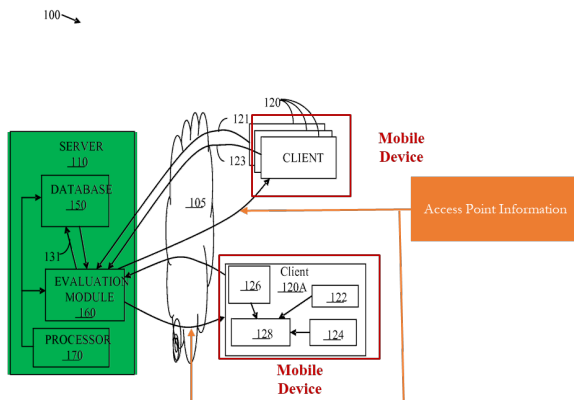


Figure 1

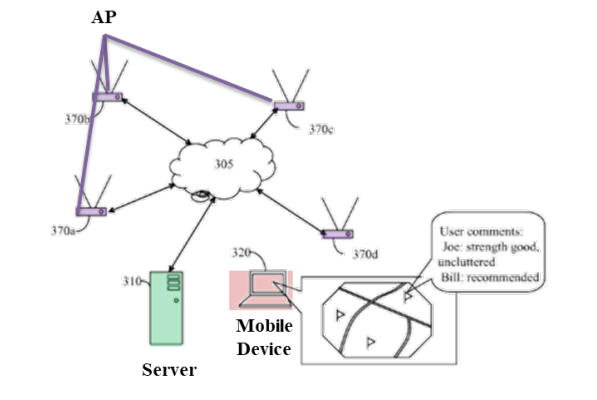


Figure 3

To the extent PO contends *Vardi*'s disclosures are not explicit, *Orava* explicitly discloses all four. EX1005, ¶¶[21] (“**MT** comprises at least memory, a [2-4] *transceiver* for arranging wireless communications, and [1] a *central processing unit CPU* comprising one or more *processors*.”), [30] (“*random number generator*”); See limitations 10[a]-[d]; Bims, ¶¶584-597.

To the extent PO contends that *Vardi*'s disclosure is not explicit, *Orava* explicitly discloses “a transceiver for arranging wireless data communications.” ¶[21]; Bims, ¶¶584-597. EX1008, 3 (“Transceiver: A device that can both transmit and receive signals.”); Bims, ¶¶584-597.

- h. 24[e]: “a memory to store the information regarding the at least one access point, and the authenticated access point list; and”

Vardi-IEEE802.11-Orava-Yun render obvious limitation 24[e] See limitation 10[d] and claim 13; EX1007, 7:31-32 (“user’s clients can store some or all of this information in the memory of the wireless user terminal to a... wireless access point

to connect to.”); EX1005, ¶[21] (“**MT** comprises at least memory”) ; Bims, ¶¶598-600.

- i. 24[f]: “*a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,*”
- j. 24[g]: “*wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and*”

Vardi-IEEE802.11-Orava-Yun render obvious limitations 24[f-g]. Bims, ¶¶601-606. Limitations 24[f-g] differs from limitation 10[e] in that it adds a “determination unit to determine” the same steps. See limitation 10[e] and 24[f-g].

Vardi discloses the determination unit. Bims, ¶¶601-606. Specifically, *Vardi* discloses “**wireless user terminal** can be a device that *executes* a program (e.g., a **client**)... The client can be a software program *executed* on the **wireless user terminal**,” the claimed “determination unit... under control of the processor.” 7:10-20; Bims, ¶¶601-606. *Vardi*’s **client** determines whether the **AP** is the **preferred AP**—an authenticated access point—comparing the stored **API** with the **API** received from an IEEE802.11 scan. See limitations 10[a], 10[d], 10[e]; EX1007, 14:52-57.

To the extent PO contends *Vardi*'s processor is not explicitly disclosed, as explained in limitation 24[a], it would have been obvious to implement *Orava*'s processor as part of *Vardi*'s mobile device to execute the client software performing the determination whether the AP is the preferred AP. Bims, ¶¶601-606.

- k. 24[h]: *“wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.”*

Vardi-IEEE802.11-Orava-Yun render obvious limitation 24[h]. Bims, ¶¶607-609. Limitations 24[h] adds nothing more to claim 10 than a well-known mobile device component—a “transmitter.” See limitation 10[f] and 24[b-c]; Bims, ¶¶607-609. As explained above, for limitations 24[b-c], *Vardi* and *Vardi-Orava* disclose the claimed “transmitter.” And as explained in limitation 10[f], *Vardi-IEEE802.11-Orava-Yun*'s **mobile device** transmits a connection request to the determined **preferred AP**. See limitation 10[f]; Bims, ¶¶607-609.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.

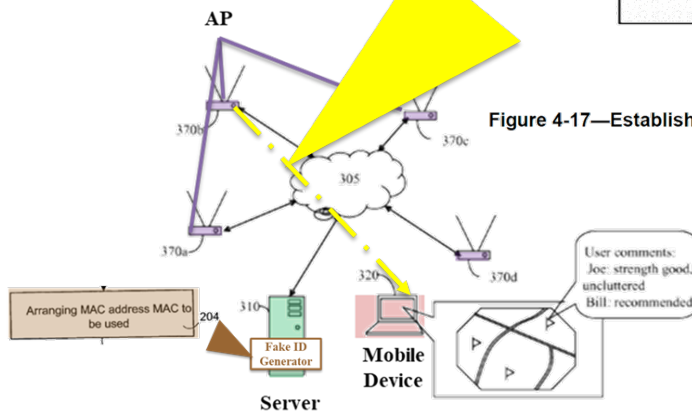
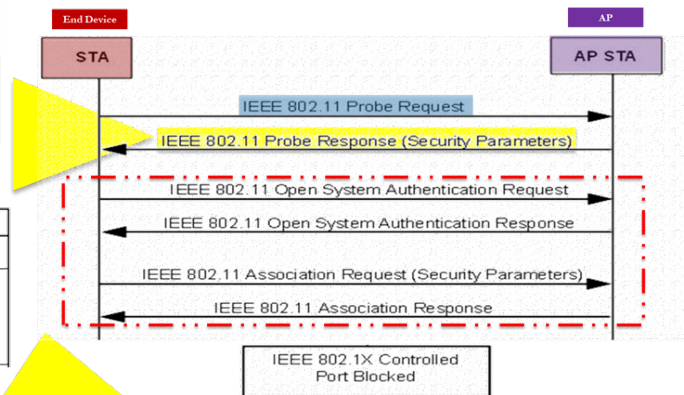


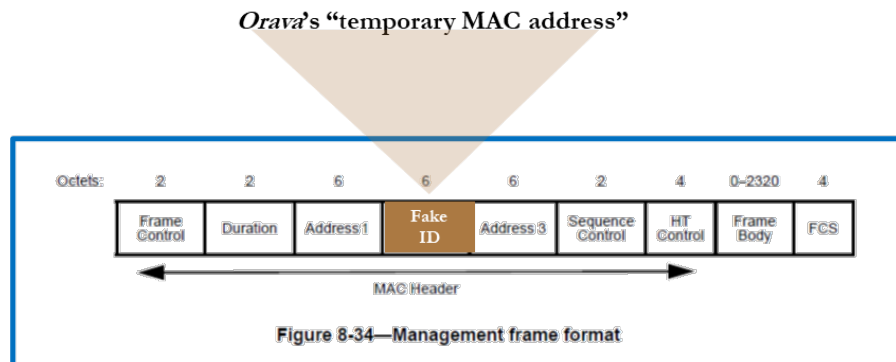
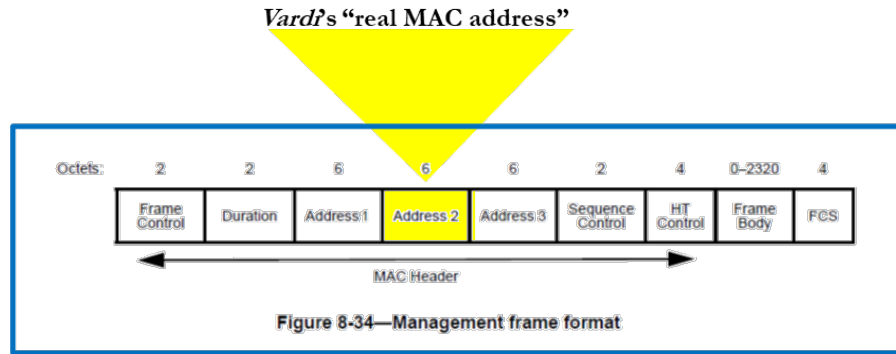
Figure 4-17—Establishing the IEEE 802.11 association

Figure 3

16. Claim 25: “The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.”

Vardi-IEEE802.11-Orava-Yun render obvious claim 25. Bims, ¶¶610-613.

See, limitation 10[b] and claim 11; Bims, ¶¶610-613.

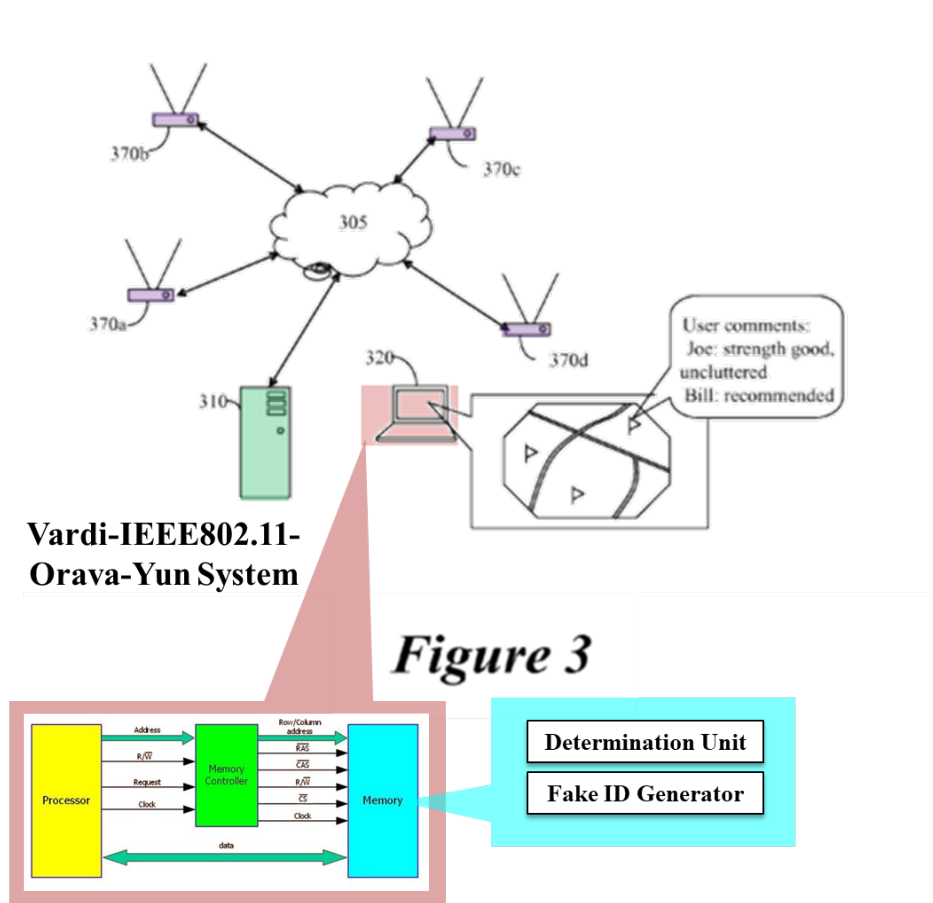


17. Claim 26: *"The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier."*

Vardi-IEEE802.11-Orava-Yun render obvious claim 26. Bims, ¶¶614-618.

Vardi-Orava teaches "a fake device identifier generation unit to generate, under control of the processor, the fake device identifier." See, limitations 10[b] and claims 11 and 24; Bims, ¶¶614-618. Dependent claim 26 and limitations 10[b] and claim 11 differ only by the inclusion of a "generation unit, under control of the processor." *Vardi-Orava*, however, teaches that the mobile device includes a "CPU comprising one or more processors," the "Computer program codes executed in the [] CPU can cause the terminal MT to implement inventive means, some embodiments of which are illustrated in FIGS. [2-7]," the claimed "generation unit

under control of the processor.” EX1005, ¶[30], EX1007, FIG. 3-EX1005, ¶[21]; Bims, ¶¶614-618.



18. Claim 27: “The system of claim 24, wherein the memory further stores the fake device identifier.”

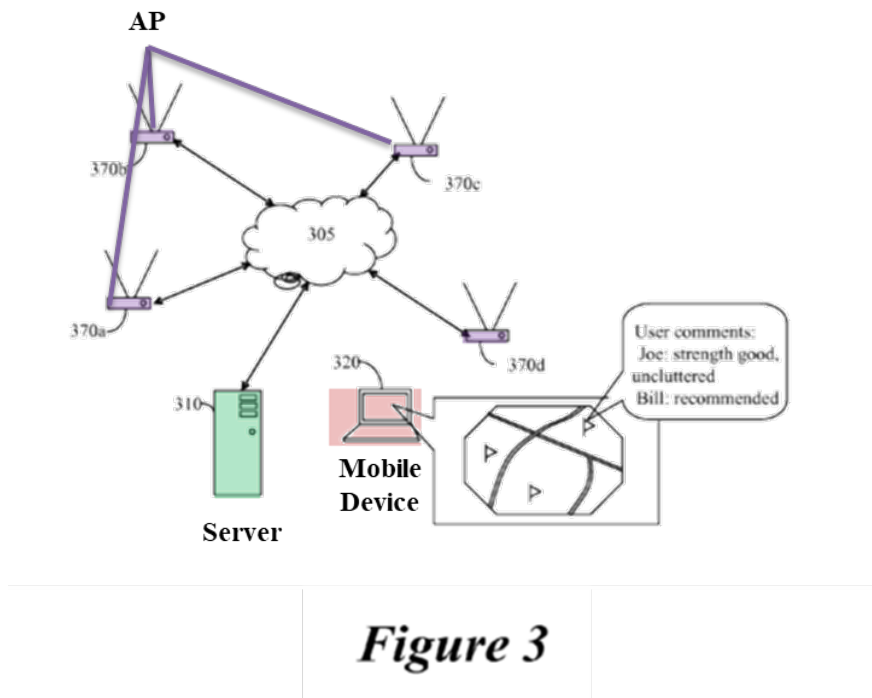
Vardi-IEEE802.11-Orava-Yun render obvious claim 27. Bims, ¶¶619-624.

See limitations 10[b], 21[b] and claim 23; Bims, ¶¶619-624.

19. Claim 28: “*The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.*”

Vardi-IEEE802.11-Orava-Yun render obvious claim 28. Bims, ¶¶625-632.

Vardi discloses the APs provide Wi-Fi. EX1007, 14:66-15:1 (“FIG. 3... radio access points 370a-d are connected to a network 305, such as the Internet.”); 7:6-43. Additionally, *Vardi-Orava*’s mobile devices are configured to communicate via *Wi-Fi* with the APs. EX1007, 9:54-59 (“clients continuously collect radio resources information about APs detected by the wireless user terminal. These clients can be executed on laptops, handheld devices (PDA’s), cellphones, or any other devices that *incorporates a radio facility for wireless communication*, such as *WiFi*.”); 5:11-16 (“Wifi enabled mobile telephones”); 7:36-40; FIG. 3.



As explained above, *Vardi* discloses the claimed “communication interface”; however, to the extent PO contends that *Vardi*’s disclosure of a communication interface is not explicit, it would have been obvious to combine *Orava*’s communication interface comprising a transceiver with *Vardi*’s mobile device. See limitation 24[b]; EX1005, ¶¶[19] (“FIG. 1 shows a telecommunications system... the system comprises a **terminal device MT** and a WLAN network WLAN according to any version of the IEEE802.11 standard.”); [21](“**MT** comprises... a transceiver...”); FIG. 1; Bims, ¶¶625-632.

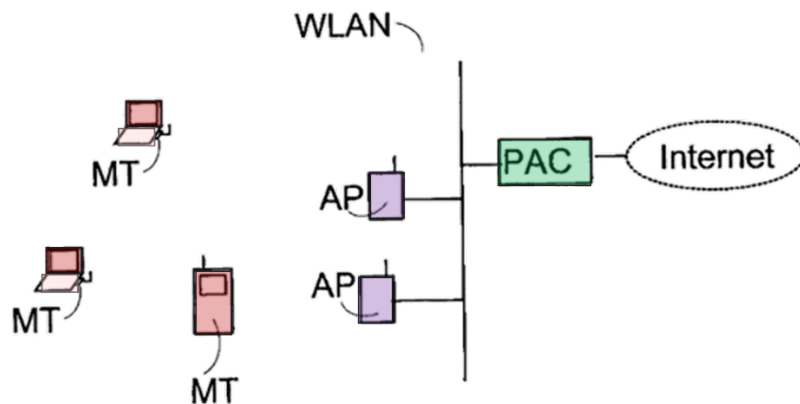


Fig. 1

B. Ground 2: 24-28 Are Obvious over *Vardi* in combination with *IEEE802.11*, *Orava*, and *Kholaif*

Should the PO contend that *Vardi*’s or *Orava*’s disclosures of certain hardware elements identified by claim 24 and its dependent claims 25-28 are not explicitly disclosed, combining the *Vardi-IEEE802.11-Orava-Yun* system with *Kholaif* renders obvious claims 24-28.

A POSITA at the time of the alleged invention reading *Vardi* knows that “clients [] executed on laptops, handheld devices (PDA[s]), cellphones, or any other devices that incorporate[] a radio facility for wireless communication, such as WiFi...” discloses the claimed “processor,” “at least one communication interface” (e.g., transmitter/receiver for “WiFi”) “transmitter,” “receiver,” “memory,” and “determining unit” (e.g., processor executing software (“client”)). EX1007, 9:54-62; Bims, ¶¶584-609.

Furthermore, the *Vardi-IEEE802.11-Orava-Yun* combination explicitly teaches the claimed hardware. EX1005, ¶¶[21], [30]; Section IV.A.6.a. Bims, ¶¶584-609. Nonetheless, *Kholaiif* provides an explicit disclosure and illustration of the internals to support further that these components were well-known. EX1010, FIG. 27. Bims, ¶¶643-649.

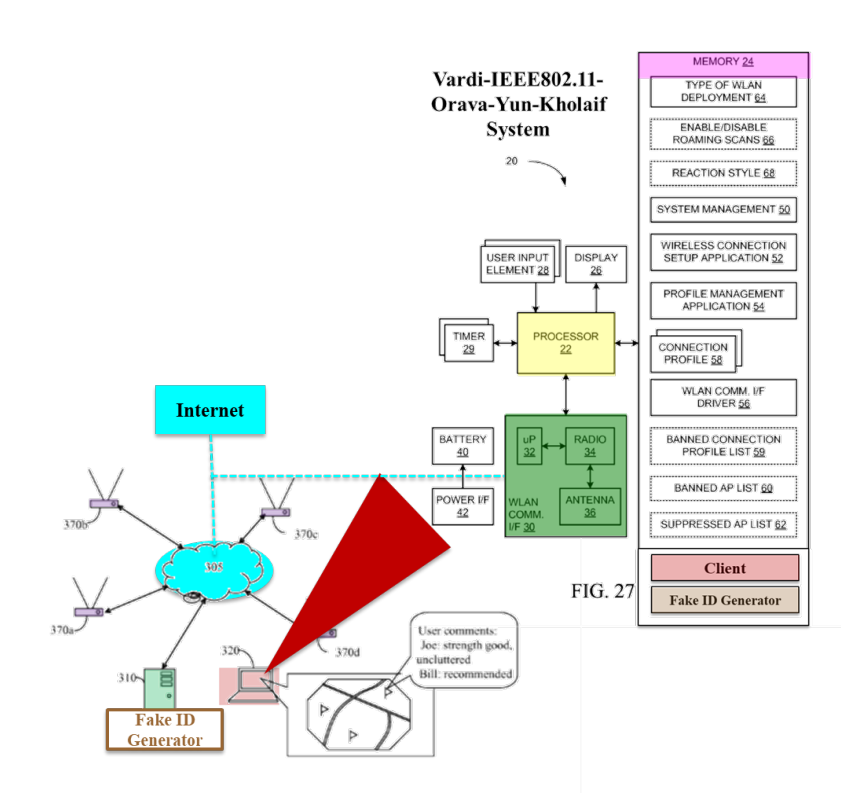


Figure 3

1. Independent Claim 24

a. 24[pre-e]

Vardi-IEEE802.11-Orava-Yun-Kholaif render obvious limitations 24[pre] (to the extent its limiting) and 24[a –e]. Limitations 24[pre] and 24[a-e] add nothing more to claim 10 than well-known mobile device components: (1) processor; (2) communication interface; (3) transmitter; (4) receiver, and (5) memory to perform the method steps of claim 10. Bims, ¶¶643-645. Each of these well-known mobile device components and corresponding claimed operations are disclosed by *Vardi-IEEE802.11-Orava-Yun* as detailed above in Section VII.A.15 above, however, to

the extent PO contends otherwise, *Kholaif* explicitly teaches these well-known components. Bims, ¶¶643-645.

Kholaif discloses a “mobile station...” comprising “a processor 22” and a “WLAN communication interface comprises a baseband processor coupled to a radio, which [] is coupled to an antenna.” *Kholaif* teaches a “memory to store.” ¶[55] (“mobile station may *store in its memory*...”), ¶[242] (“mobile station... comprises... a memory”), ¶[245] (“Memory is coupled to processor and comprises volatile memory and non-volatile memory.”); Bims, ¶¶643-645. EX1010, FIG. 27 (“a functional block diagram illustration of [a] mobile station.”), ¶[241]; EX1007, FIG. 3; *See* Ground 1 claims 10, 13, 24; Bims, ¶¶643-645.

As explained herein, a POSITA would have looked to and for components that support IEEE 802.11 standard communications when deploying mobile devices in a IEEE802.11 WLAN. Bims, ¶¶124-130.

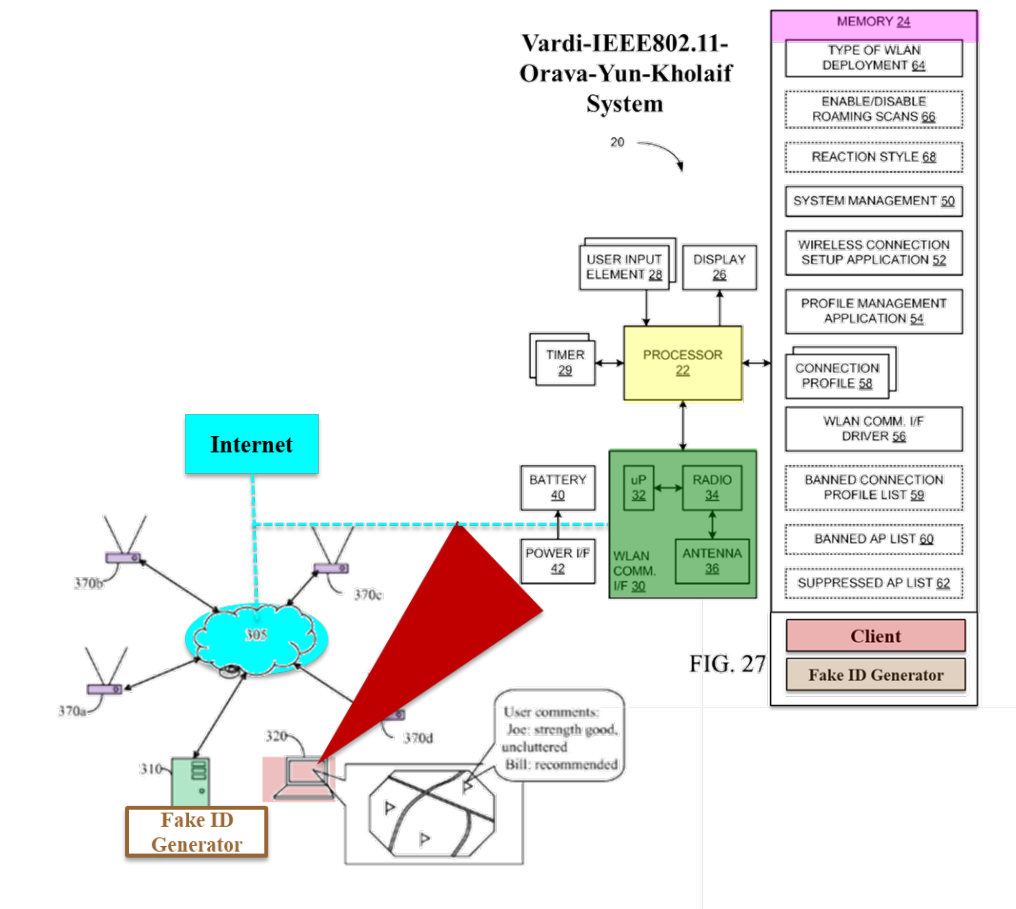


Figure 3

b. 24[f-g]

Vardi-IEEE802.11-Orava-Yun-Kholaif render obvious limitations 24[f-g]. Bims, ¶¶646-648. Limitations 24[f-g] differs from limitation 10[e] in that it adds a “determination unit to determine” the same steps. See limitation 10[e] and 24[f-g].

To the extent that PO contends *Vardi-IEEE802.11-Orava-Yun*’s processor is not explicitly disclosed, as explained in limitation 24[a], it would have been obvious to implement Kholaif’s processor as part of *Vardi*’s mobile device to execute the

client software performing the determination whether the AP is the preferred AP.

Bims, ¶¶646-648.

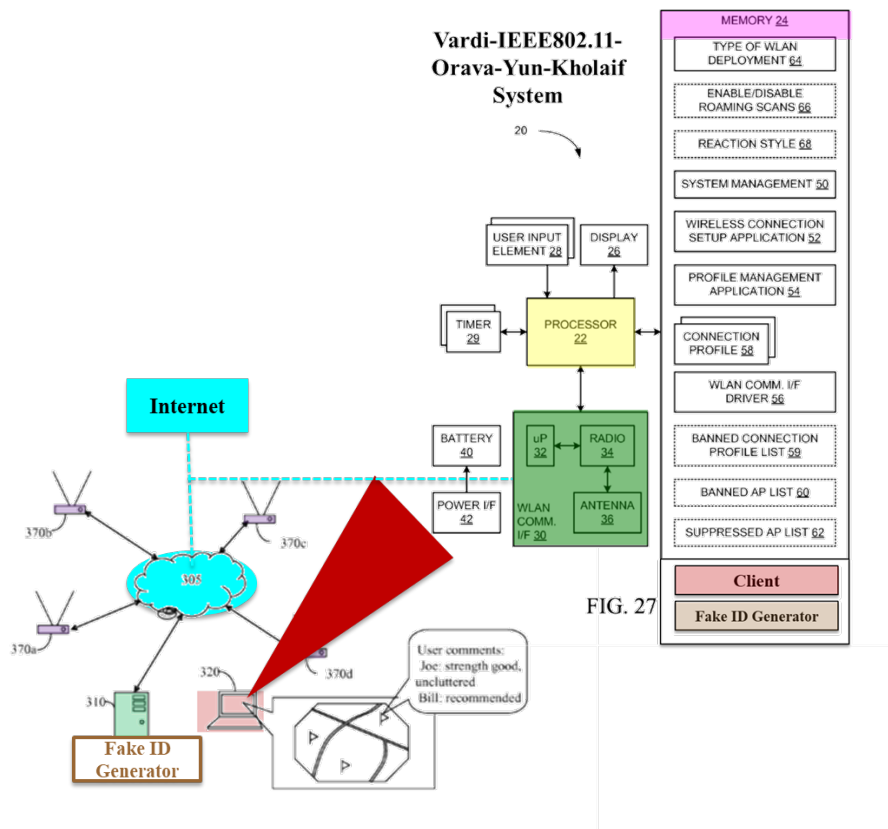


Figure 3

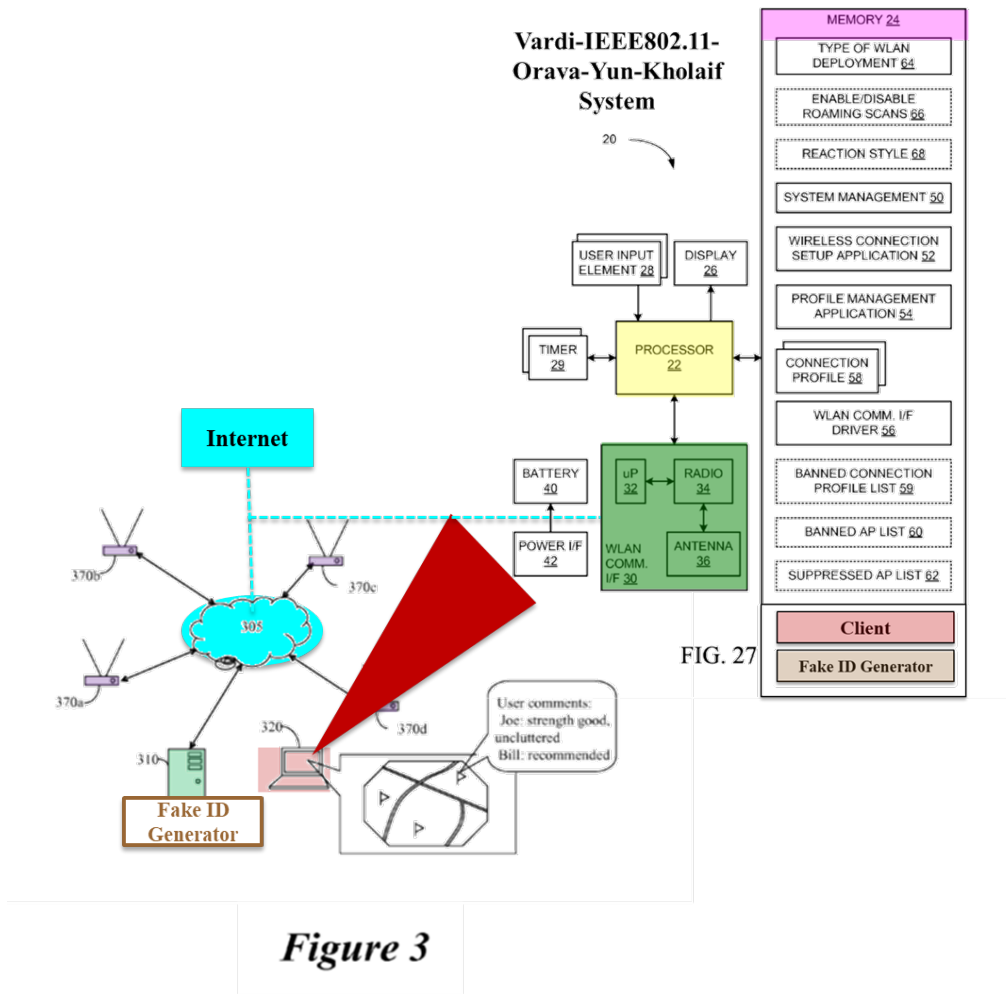
c. 24[h]

Vardi-IEEE802.11-Orava-Yun-Kholaif render obvious limitation 24[h]. As explained in limitation 24[c], Kholaif teaches a “transmitter.” See limitation 24[c], EX1010, ¶[242], FIG. 27; Bims, ¶649.

2. Claim 25–Claim 27

Vardi-IEEE802.11-Orava-Yun-Kholaif render obvious claims 25-27. Bims, ¶¶650-654. As explained above, *Vardi* or *Vardi-Orava* teaches or at least renders

obvious the processor executes software, (the claimed generation unit under control of the processor), that randomly generates a Fake ID that is in IEEE MAC address format and stored in memory. See limitations 10[b], 21[b]; EX1005, ¶¶[21] (“terminal MT comprises [] memory... and a [] CPU comprising one or more processors... Computer program codes executed in the [] CPU can cause the terminal MT to implement inventive means...”), the MT’s processor generates “MAC” [30] (“MAC can be a random number generated... [in] IEEE 802 MAC address format... in which there are 46 available bits in a 48-bit address format for selecting the temporary MAC address.”); Bims, ¶¶650-654.



3. Claim 28

Vardi-IEEE802.11-Orava-Yun-Kholaif render obvious claim 28. EX1007, FIG. 3; EX1010, FIG. 27; See claims 2 and 5; Bims, ¶¶655-658. *Vardi-IEEE802.11-Orava-Yun-Kholaif* provides wireless access via a Wi-Fi network (e.g., the Internet 305) via the AP and mobile device communication interface. EX1007, 14:66-15:5 (“The user generally is able to access the Internet 305 by connecting device 320 to access points 370d wirelessly.”); EX1010, ¶[47] (“AP 12... and AP 128 jointly support a WLAN.”); Bims, ¶¶655-658.

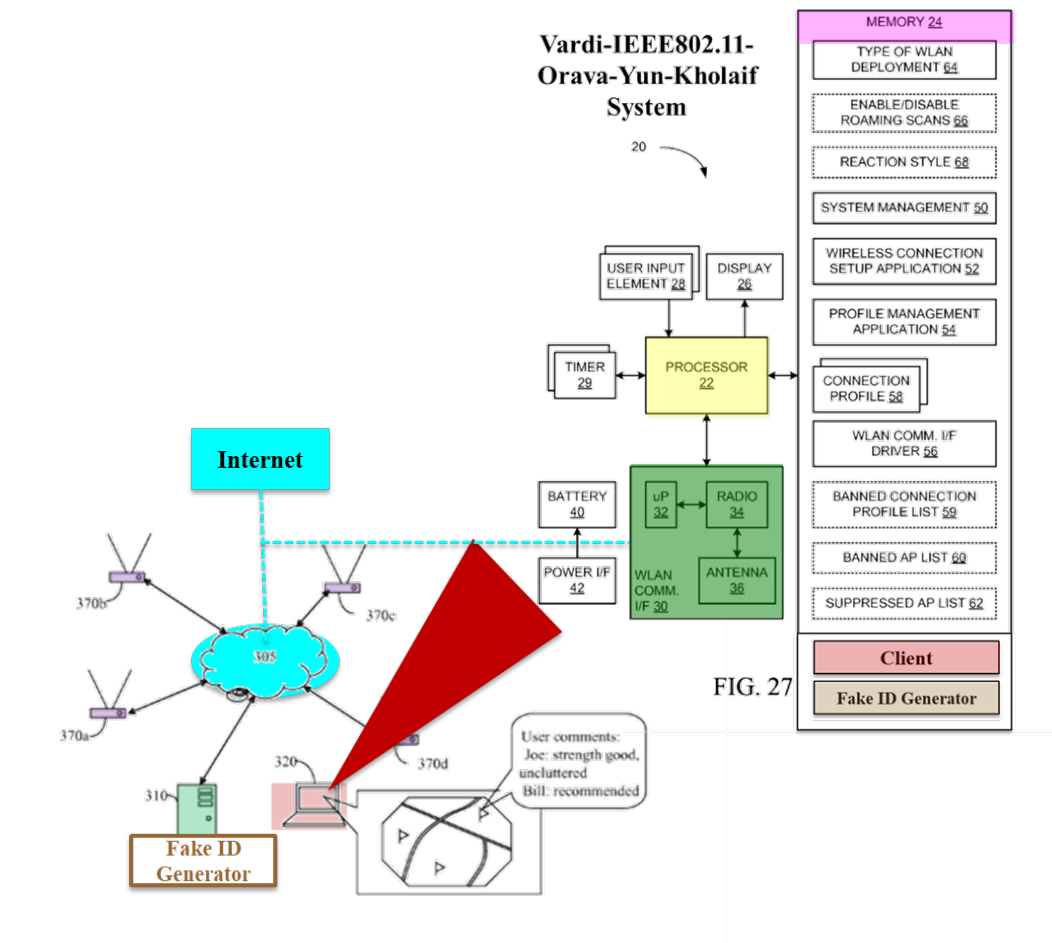


Figure 3

VIII. DISCRETIONARY DENIAL IS NOT APPROPRIATE

A. The Board Should Not Decline Institution Based on Fintiv

The Board should not exercise its discretion under § 314(a) to deny institution in view of the Texas Litigation (see Mandatory Notices, *infra*) because the balance of the Fintiv factors discussed below weigh in favor of institution.

Fintiv Factor 1 (likelihood of a stay) is neutral. There are three patents at issue in the Texas Litigation (the '552, the '005 and the '384 patents). Petitioner is

simultaneously challenging all claims of all patents in IPR. Institution of the four IPR petitions would thus enable the Board to resolve core issues in, if not completely moot, the Texas Litigation. As such, the District Court likely would stay the case pending the outcome of the IPRs in view of potentially substantial judicial efficiencies to be gained. Indeed, Judge Gilstrap (who is presiding over the Texas Litigation) granted a stay in a similar patent infringement case where all claims of the asserted patent, including the non-asserted claims, were subject to IPR. *Comm'ns Techs., Inc. v. Samsung Elecs. Am., Inc.*, No. 2:21-cv-00444-JRG (E.D. Tex. Feb. 2, 2023). Thus, this factor is neutral or slightly weighs in favor of Petitioner.

Factor 2 (proximity of trial date to IPR deadline) weighs slightly in favor of denial. The District Court tentatively set trial in the Texas Litigation for November 3, 2025, but “scheduled trial dates are unreliable and often change” so “[a] court’s schedule trial date, therefore, is not by itself a good indicator of whether the district court trial will occur before the statutory deadline for a final written decision.” *See* Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (“Vidal Memo”) at 8.

Factor 3 (investment in parallel proceeding) weighs against discretionary denial. The Texas Litigation is in its early stages. The parties have only exchanged preliminary infringement and invalidity contentions and associated document

productions. Discovery is just beginning, and the parties are yet to file any dispositive motions, exchange terms or brief Markman, or even conduct expert discovery. Therefore, the lack of investment between the parties and the court in the Texas Action is minimal and does not favor discretionary denial.

Factor 4 (overlap between issues) weighs against discretionary denial. Petitioners stipulate that, if IPR is instituted, Petitioners will not pursue in the Texas Litigation the same grounds asserted in this Petition. This “mitigates to some degree the concerns of duplicative efforts.” *See Sand Revolution II, LLC v. Continental Intermodal Group—Trucking LLC*, IPR2019-01393, Paper 24 at 12 (P.T.A.B. June 16, 2020). Moreover, this Petition challenges *all* claims not just the Asserted Claims, such that their validity will not be addressed at all in that proceeding. This factor thus weighs against discretionary denial.

Factor 5 (same parties) weighs slightly in favor of denial because Petitioners and Patent Owner are the same parties in both this proceeding and in the Texas Litigation (as is common in most IPR proceedings). Although Petitioner and PO are the parties in the Texas Action, the exceptionally strong merits presented herein warrant the Board to not discretionarily deny institution.

Factor 6 (other circumstances impacting discretion) weighs against discretionary denial. As discussed above, the key references disclose the sole alleged distinction between the admitted prior art and the claimed invention (fake

identifier during probing). *See* EX1001, 3:4-18 (describing problem with IEEE). The asserted prior art thus heavily weighs against denial because the merits are so clear.

Overall, four factors weigh against discretionary denial, and two factors weigh slightly in favor of discretionary denial. On balance, therefore, the Fintiv factors weigh against denial.

B. The Board Should Not Decline Institution Based on General Plastic

As discussed below, every General Plastic factor either weighs against the Board’s exercise of discretion to deny institution or is neutral.

Factor 1 (multiple petitions by the same petitioner) weighs against discretionary denial. The ’552 patent is not the subject of any other IPR except the IPR filed concurrently by Petitioner; however, there is no overlap in claim scope. This IPR challenges claims 10-28 while the concurrent IPR challenges claims 1-9.

Factors 2, 4, and 5 (diligence) are all irrelevant and thus neutral because no party—including Petitioner—has filed another IPR against the ’552 patent.

Factor 3 (roadmap) weighs against discretionary denial. Petitioners could not have “tailor[ed] [their] arguments to address issues identified by” the PO or Board because there are no other proceedings.

Factor 6 and 7 (finite resources and time constraints) weigh against discretionary denial. There is only one other IPR petition challenging the ’552 patent

(filed concurrently). That IPR challenges a different set of claims [1-3 (server side) and 4-9 (access point side)]; however, there are only a total of 3 grounds between the two IPRs—two here and one ground in the concurrently filed IPR. Ground 1 here and the only ground in the concurrently filed IPR present the same combination of references. Overall, therefore, this Petition is highly streamlined and requires the Board to analyze a relatively small number of claims, prior art references, and grounds, such that the additional burden on the Board is not unreasonable, and these factors weigh against discretionary denial.

In sum, Factors 1, 3, 6, and 7, all weigh against discretionary denial, while Factors 2, 4, and 5 are irrelevant and therefore neutral. On balance, the *General Plastics* Factors weigh against discretionary denial.

C. The Board Should Not Decline Institution Pursuant to §325(d)

The Board should not deny this Petition under § 325(d) because the IPR presents prior art not previously before the Office.

IX. CONCLUSION

For the reasons set forth above, Petitioner has established a reasonable likelihood that the challenged claims are unpatentable. Petitioner requests institution of *inter partes* review and cancellation of each challenged claim.

Respectfully submitted,

Dated: September 4, 2024

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr., Lead Counsel
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-4847
Fax: (202) 478-0914
Email: walter.davis@blankrome.com

Counsel for Petitioner

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for Petitioner certifies that the document contains 13,375 words in 14-point Times New Roman font, excluding the parts of the document that are exempted by 37 C.F.R. §42.24(a)(1), according to the word count tool in Microsoft Word.

Dated: September 4, 2024

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-2200

Counsel for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2024, a true and correct copy of the foregoing *PETITION FOR INTER PARTES REVIEW* including exhibits was filed with the Patent Trial and Appeal Board Case Tracking System (P-TACTS) and served via overnight FedEx to the Patent Owner at the correspondence addresses of record as follows:

154241 – IP Spring – AI
161 N. Clark St.
Suite 1700
Chicago, IL
United States

A courtesy copy was also served on PO's counsel of record in the Texas Action via email.

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-2200

Counsel for Petitioner